Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 1032761, 15 pages
https://doi.org/10.1155/2018/1032761

Review Article

Towards Privacy Preserving IoT Environments: A Survey

Mohamed Seliem, Khalid Elgazzar, and Kasem Khalil

Centre for Advanced Computer Studies (CACS), University of Louisiana at Lafayette, LA 70503, USA

Correspondence should be addressed to Mohamed Seliem; mohamed.seliem1@louisiana.edu

Received 9 July 2018; Accepted 30 October 2018; Published 18 November 2018

Guest Editor: Constantinos Kolias

The Internet of Things (IoT) is a network of Internet-enabled devices that can sense, communicate, and react to changes in their environment. Billions of these computing devices are connected to the Internet to exchange data between themselves and/or their infrastructure. IoT promises to enable a plethora of smart services in almost every aspect of our daily interactions and improve the overall quality of life. However, with the increasing wide adoption of IoT, come significant privacy concerns to lose control of how our data is collected and shared with others. As such, privacy is a core requirement in any IoT ecosystem and is a major concern that inhibits its widespread user adoption. The ultimate source of user discomfort is the lack of control over personal raw data that is directly streamed from sensors to the outside world. In this survey, we review existing research and proposed solutions to rising privacy concerns from a multipoint of view to identify the risks and mitigations. First, we provide an evaluation of privacy issues and concerns in IoT systems due to resource constraints. Second, we describe the proposed IoT solutions that embrace a variety of privacy concerns such as identification, tracking, monitoring, and profiling. Lastly, we discuss the mechanisms and architectures for protecting IoT data in case of mobility at the device layer, infrastructure/platform layer, and application layer.

1. Introduction

The Internet of Things (IoT) is a group of connected physical devices that exchange data about themselves and their environments and may take actions on it. The 2017 report of the International Data Corporation [1] forecasts that 50 billion devices will be connected by 2020 with a $8.9 trillion market value. Gartner [2] published a similar study expecting that, in 2020, 50 Billion devices will have their own unique Identifier with a $19 trillion market share opportunity. Not only are IoT devices equipped with a varying level of computational power (e.g., microcontrollers) but also many run a full stack operating system (e.g., Contiki [3] and RIOT [4]) that enables these devices to perform high-level functionality.

The main strength of IoT is the huge impact it will have on several aspects of the user's everyday interactions and the surrounding environment (e.g., smart spaces). This will improve our quality of life in different domains [5] as shown in Figure 1 including Energy [6], Safety, Security, Industry [7], Environment, Entertainment, and Healthcare [8]. However, IoT devices are intrinsically resource-constrained in terms of computation, battery power, intermittent connectivity, and network protocols.

These constraints directly impact the choice of technology applicable to maintain user privacy. Hence, promoting IoT adoption from the user perspective and mitigating potential risks of data misuse and security concerns. IoT devices do not commonly implement a standard security scheme [3, 4], which means there is a huge risk to connect this large number of unsecured devices to the Internet [9]. Proofpoint Inc. has uncovered the first proven cyberattack based on IoT household smart appliances between December 23, 2013, and January 6, 2014. This attack involved more than 750,000 malicious email communications coming from more than 100,000 everyday consumer gadgets such as home routers, smart TVs, and smart refrigerators [10]. In 2015, two ethical hackers, Charlie Miller and Chris Valasek, gained control of a Jeep Cherokee remotely through vulnerability in its onboard entertainment system. According to the hackers, they were able to break the Uconnect system that the Chrysler's line-up of cars and trucks use due to open vulnerability. Hundreds of thousands of vehicles could be affected. In October 2016,

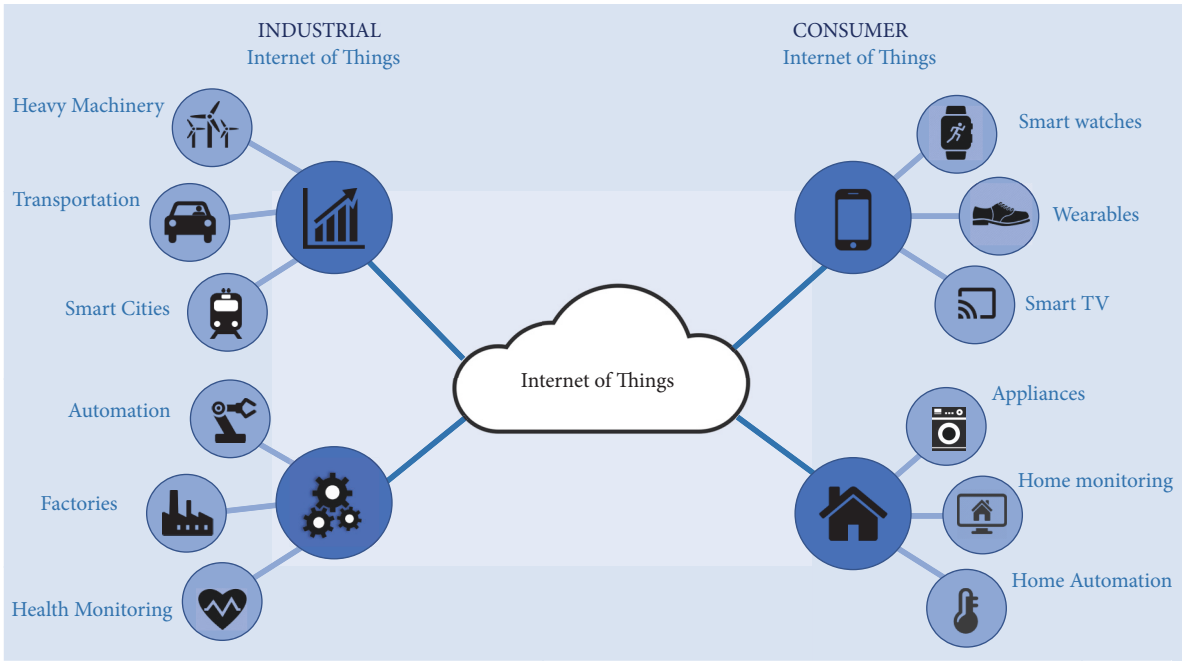

Figure 1: Internet of Things applications.

a major DDoS attack took down several giant servers such as Airbnb, Reddit, Etsy, Sound Cloud, New York Times, Amazon, Twitter, and Spotify. Though it is not clear yet that the blame is on IoT, it is quite likely.

IoT devices are considered not only a security threat, but also a major privacy concern, as these devices collect much personal data such as user identity, location, energy consumption, and telephone numbers. This information can reveal a lot about the user's daily life activities (e.g., using washing machines, watching TV, and leaving or returning home). The major concern yet is that these devices not only can collect users' private data but also can control their environments. Thus, users are highly uncomfortable exposing personal data to public or private servers without a well-established trust model [11]. Therefore, the lack of well-designed IoT-oriented privacy and security techniques will inhibit the user adoption to any IoT technology [12].

The following scenario embodies much of the semantic meaning of user privacy leakage and associated risks. Ahmed looks at his smartwatch while doing his usual workout and sees that his heart rate is a little high. Once he arrived home, he speaks to the smart speaker installed in his room to provide him a list of nearby cardiologists to check his heart and blood vessels. Next day after finishing his work, Ahmed visited a cardiologist, and he felt relieved when his doctor reassured everything is fine. "You just did more exercises than usual and nothing to worry about", the doctor said. The next day, every time Ahmed uses his browser he finds too many advertisements related to heart medication, heart monitoring devices, and many tutorials about diagnosing a heart attack and how to handle it. Things got more serious when he received a phone call from his insurance company for check-up survey. "Goodbye privacy", he whispers to himself as he speaks with the company representative. This is only one scenario of too many that shows high privacy risks associated with modern technology usage that has become an inevitable part of our everyday life.

There exist many published surveys on IoT privacy and security issues, challenges, and solutions. Ziegeldorf et al. [13] analyze the privacy issues in IoT. Their focus is on classifying the various privacy threats and pointing out the challenges in IoT scenarios. Sadeghi et al. [14] introduce the security and privacy challenges of industrial IoT systems. They also discuss possible solutions towards a complete and secure framework for industrial IoT. Sicari et al. [15] focus on the main security challenges and the current solutions. They categorize the issues into authentication, access control, confidentiality, privacy, trust, secure middleware, mobile security, and policy enforcement. Suo et al. [16] review the security and privacy in IoT, where they analyze the security architecture and features. They also discuss ongoing research status and the challenges of secure technologies including encryption mechanism, communication security, protecting sensor data, and cryptographic algorithms to support privacy preservation in IoT. Although security and privacy are highly correlated, this paper primarily focuses on privacy challenges and discusses a broad range of privacy-related aspects in open IoT environments to provide better insights on the design principles and development of privacy preserving IoT environments.

The remainder of this paper is organized as follows. Section 2 summarizes the unique characteristics of IoT posing significant challenges on resource-constrained IoT devices. We also discuss the notion of privacy in IoT by pointing out some scenarios related to privacy concerns. Section 3 describes major IoT privacy issues and concerns

such as identification, tracking, monitoring, and profiling. Then, we discuss existing IoT privacy solutions in Section 5. Section 6 provides a comprehensive analysis of privacy issues and mechanisms at the different layers of the IoT stack, namely, Device Layer, Platform Layer, and application layer, respectively. Lastly, Section 7 concludes the paper and provides closing notes.

2. Privacy in the Internet of Things

IoT provides consumers with a high degree of automation and control on how to carry out everyday tasks through saturating the environment with smart things. IoT smart things refer to a broad spectrum of nonstandard computing devices including microcontrollers, sensors, and actuators that can transmit and exchange data to enable smarter interactions and support informed decision making. Things are embedded in consumers' devices and industrial machinery to collect and exchange data about the surroundings. Things can also cause physical changes to their environments and can be controlled directly from proximity or remotely via Internet. Although privacy concerns discussed in this paper are generally valid for any IoT deployments, we provide examples related to consumers' connected devices such as smart appliances to make the point clear. In addition, the pace at which consumers' smart devices are developed is much higher than the development of safeguard techniques that can protect these devices and their data collection from growing privacy threats. Given the high penetration of IoT devices and their impact on our everyday life, we need to fully understand the risks and challenges such devices pose on our privacy. More importantly, we need to answer the following question: Is it possible to support privacy preserving and safe environment for IoT users such those offered in traditional Internet? To precisely answer this question, we need first to discriminate between relevant terminologies such as privacy, trust, and security.

Privacy means that information about individuals must be protected and should not be exposed without explicit consent under any circumstances. Every individual has the ultimate right to decide with whom to share their data. For example, in our previous scenario, Ahmed should be the only one to decide whether to share his heart conditions with the insurance company or not.

Trust is defined as the product of attack probability and the damage it can cause. Trust is derived from two crucial terms: transparency and consistency. Transparency means that IoT devices collecting information inform the user about what data is collected, the purpose of collection, and how the collected data will be used. Consistency means that the behaviour of IoT devices consistently meets user expectation. For example, if a user asks his smart speaker to control the room light, it must do nothing unintended, but the specific requested task. Security refers to the protection of devices and connection from unauthorized access.

Based on the aforementioned definitions, it is evident that privacy is more general than both security and trust. For instance, an IoT service could gain user trust and provide proper security but still violates the user's privacy by exposing personal data without clear and explicit permissions.

Table 1: List of top countries with vulnerable IoT devices.

Country	# of vulnerable devices
United States	57,598
China	17,455
Germany	17,273
France	10,708
India	9,427
United Kingdom	9,268
Russian Federation	7,897
Korea	7,525
Brazil	7,095
Japan	5,302

2.1. Impact of Device Limitations on Privacy. IoT smart things are typically resource-constrained with limited capabilities due to size and weight (e.g., memory, processing, and battery power) and network connectivity (e.g., IEEE 802.15.4). For example, IEEE 802.15.4 specification is constrained with respect to (1) low data rates, which range from 20 Kbits/s (868 MHz) to 250 Kbits/s (2.45 GHz), (2) unreliable and lossy links compared to wired links, (3) small packet size (127 bytes), which means less room for payload when including other headers, and (4) aggressive power cycle, by which IoT smart things aim to save power by staying longer in low-power mode. Such constraints directly impact the type and complexity of functionality that IoT devices can run.

Recently, significant efforts have been made towards standardizing the IoT protocol stack [17]. For example, to enable low-power connectivity among smart objects in IoT systems, the IEEE 802.15.4–2006 low-power physical (PHY) layer and the IEEE 802.15.4e link layer based on Time Synchronized Channel Hopping (TSCH) have been developed in 2006 [18]. Several scholars pointed out the technical challenges that face IoT environments due to various resource constraints.

Yu et al. [19] consider IoT devices as weak access points to vital infrastructures (e.g., a medical or military facility) and can be misused to leak sensitive data. The authors have made two main observations regarding IoT systems: (1) network-based approaches are less vulnerable than host-based approaches due to inherent limitations and possible unpatched vulnerabilities on IoT devices; (2) traditional static perimeter defenses are unable to secure IoT devices, since these devices are deployed deep inside the network, with their physical and computational context constantly changing. Therefore, resource limitations make it challenging to secure IoT layers individually. Table 1 lists the top countries, in Sept 2017, with IoT devices (237,539 devices) vulnerable to Heartbleed [20] according to SHODAN [21] and other sources.

2.2. Impact of Complex Heterogeneity on IoT Privacy. IoT has intrinsic complexity, since multiple diverse objects located

in different contexts can exchange information among each other. This complicates the design and deployment of efficient, interoperable, and scalable mechanisms to preserve users' privacy. Heterogeneity also has significant influence on the design of IoT protocols. Recourse-constrained devices will interact with one another/infrastructure (e.g., web servers and cloudlets) either directly or through gateways. In this case, it is essential to implement or create lightweight security protocols that support an end-to-end secure communication channel. These protocols require implementing distributing management system to distribute credentials and facilitate keys session establishment between peers.

The data flooding caused by billions of IoT devices is a big threat, in a way that hurts and violates the user's privacy. One of the main violations of the large volume of data exchange is linking this data to a certain user. So, the user's anonymity is another dimension that must be taken into consideration to support privacy in connected environments. Further, creating mechanisms to provide data summarization and access policies related to private data will enable transparency and avoid IoT silently taking control of our lives.

There exist several surveys focusing on the impact of IoT heterogeneity on users' privacy. Heer, T. et al. [22] provide a number of requirements to secure IoT environments and preserve user privacy through overcoming specific technical limitations including (1) complex heterogeneity of IoT systems, which complicates protocol design and system operation; (2) scarce CPU and memory resources, which limit the use of resource-demanding cryptoprimitives, such as public-key cryptography as used in most Internet security standards; and (3) end-to-end security measures that are IoT-oriented, since traditional Internet-based approaches are typically inapplicable due to resource limitations. The lessons we learned so far suggests that resource limitations are a major inhibitor to the adoption of traditional techniques as is. IoT architectures must implement privacy by design from the ground up [23], to provide users with central control over their security and privacy.

3. Motivating Scenarios

The vulnerabilities of IoT devices can lead to huge security breaks and threaten user privacy by exposing vital personal information. In this section, we provide some scenarios of IoT applications where personal data can be breached.

3.1. Smart Home Utility Monitoring. According to a recent report published by US Energy Information Administration (EIA) in 2017 [24], 64.7 million smart meters have been installed in electric utilities in 2015. Around 88% of these installations were residential upgrades as shown in Table 2. These smart meters measure and log electricity usage at a minimum of 1-hour intervals but can report readings in real-time at a much higher sampling rate. This data is collected by utility companies at least once a day. Smart meters range from basic hourly interval meters to real-time meters equipped with two-way communication that is capable of recording and transmitting instantaneous data. Natural gas meters and water meters are also on the rise and likely count to similar numbers. However, EIA does not publish their data publicly. The extensive deployment of smart meters has serious privacy implications since they unintentionally leak detailed information about residents' activities. Processing and analyzing this information can lead to serious privacy leakage such as profiling the behaviour of the residents. Furthermore, with existing sophisticated analytics such data may reveal when residents are home and what may be their heath conditions (e.g., toilet flushing rate may indicate that the resident has diarrhoea). This does not stop at breaking the user privacy but may very much lead to life-threating situations.

Table 2: Number of AMI installations by sector, 2015.

Sector	# of smart meters
Residential	57,107,785
Commercial	7,324,345
Industrial	310,889
Transportation	813

Molina-Markham et al. [25] raise awareness around privacy issues related to the use of smart meters. They show that even without knowing any information about household activities, applying off-the-shelf statistical methods can easily extract complex usage patterns from smart meter data. Their work is based on data collected over a 2-month period from three homes. The data contains household power consumption aggregated at 1-second rate. Even with this small-scale deployment, the authors managed to demonstrate the latent for power consumption patterns to reveal a range of personal information, such as how many people are in the house, sleeping routines, and eating routines. The proposed privacy-enhancing smart meter is based on 3 components: household smart meters, neighbourhood gateways, and a remote utility server. The server applies Zero-Knowledge (ZK) protocols [26] that allow a prover (smart meter) to demonstrate the knowledge of a secret (collected data) to a verifier (gateway/server), without revealing any information that help the verifier to infer the secret. This enables utility companies to accomplish their goals without compromising the customer's privacy.

Apthorpe et al. [27] discuss the same concern. However, they point out that an Internet Service provider (ISP) or other network observers can gather private and sensitive information about home activities by analyzing Internet traffic from smart homes containing IoT devices even if the devices use secure encryption. Several strategies have been investigated to avoid the privacy risks associated with smart home traffic monitoring such as traffic blocking, tunnelling, and rate-shaping. However, the user cannot block outgoing traffic from their home; otherwise their devices will be unusable. While traffic tunnelling via a VPN is more secure, it does not totally guarantee privacy preserving. Authors propose the use of traffic shaping using Independent Link

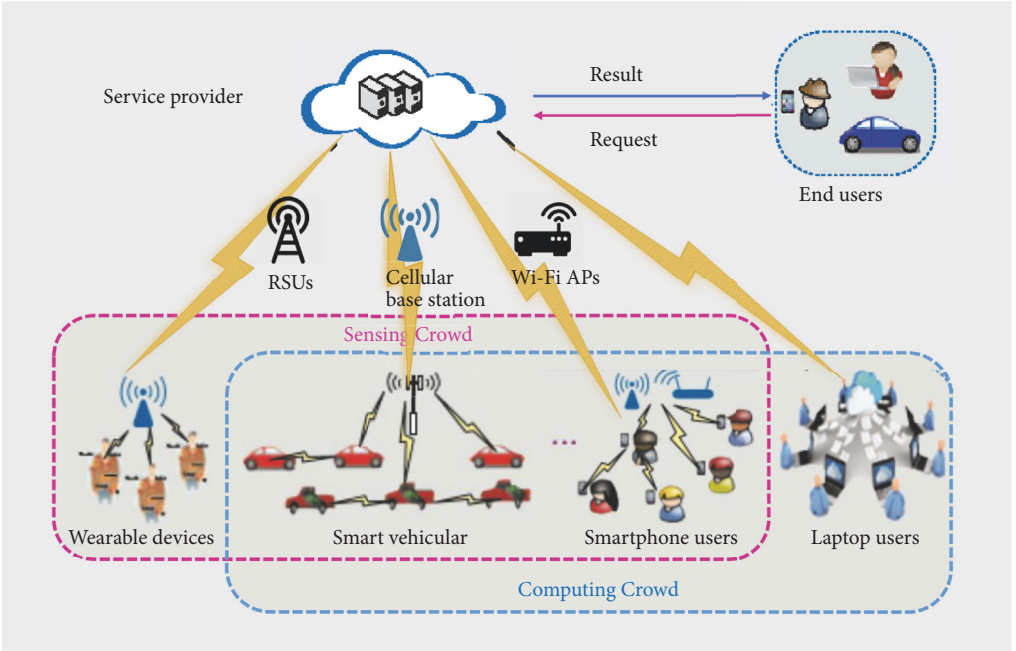

Figure 2: General architecture of mobile crowdsourcing networks (reproduced from [28]).

Padding (ILP) to prevent the leak of rate information and thus render attacks impossible.

3.2. Crowdsourcing and Public Monitoring. Crowdsourcing is the use of collective knowledge of a large crowd to help solving a specific problem. Crowdsourcing benefits from high penetration of smartphones, which becomes the common mobile platform for users worldwide.

Developers and average users with limited programming experience can create feature-rich/personalized applications by simply requesting access to private information such as location, contact lists, media files, etc. However, this model raises serious privacy concerns with no trust mechanisms that govern how applications access and handle such private information. It is also technically possible that applications may gain unauthorized access to the device's camera, networks, and system settings. Mobile Crowdsourcing Networks (MCN) include four basic types of entities as depicted in Figure 2:

(i) The service provider is a crowdsourcing platform that offers crowdsourcing services to both end users and public crowds.

(ii) End users are the clients who purchase or rent crowdsourcing services at a certain cost.

(iii) Sensing crowd is a crowd of mobile users who accept and participate in crowdsourced sensing tasks.

(iv) Computing crowd is a crowd of users who accept and participate in crowdsourced computing tasks (sensing-based computing tasks, or pure computing tasks).

Yang et al. [28] point out that the privacy may be leaked out from either data or tasks. Privacy threats resulting from data leakage can be divided into three categories. (1) privacy of sensed data contains personal information about participants, such as identities, location information, and biometric information. For example, the location information can be easily obtained either from GPS receivers embedded in mobile devices or triangulation-based approaches on Wi-Fi or cellular networks. Moreover, environmental context such as ambient temperature, light, noise level may also reveal the location information. The disclosure of the location information may leak the privacy of participants, such as home and workplace locations, routines, and habits. (2) Privacy of crowdsourced data may contain sensitive information, such as business and financial records, proprietary research data, or personal health information. (3) Privacy of crowdsourcing results can be analyzed to infer sensitive information not authorized/known by the service provider.

4. Evaluation of Privacy Threats in IoT

IoT increasingly evolve with new emerging technologies and services. In this section, we discuss the various privacy threats and challenges associated with IoT environments. We provide a solid definition and a concrete example of privacy violation for each threat. Then, we discuss the impact of IoT evolution on this threat. Lastly, we point out the main challenges associated with these threats as well as any correlation when exists.

4.1. User Identification. From privacy perspectives, user identification is the ability to distinguish a person (or an entity) or revealing their identity based on a piece of acquired data

(e.g., name, address, or personal information). The risk of such a threat is that privacy-violating actions could be carried out after the customer is identified. This threat enables and aggravates other threats, e.g., profiling and tracking of individuals' behaviour. It also allows for linking information from different sources for the same identified target. Analyzing this information can easily result in exposing the target's life pattern. For example, developers that have access to user traces can utilize machine learning techniques to infer personal information about users' interests, which can be exploited to flood user interfaces with ad-ware and targeted advertisements.

The wide adoption of IoT facilitates the collection of a huge amount of data using IoT devices that can be stored and analyzed beyond the user's control domain. Thus, user identification becomes the dominant threat regarding user's privacy. Further, with the increasing number of IoT deployments, the user identification threat and associated risks will significantly scale up.

Different IoT technologies bring their own benefits and challenges. Radio Frequency Identifier (RFID) is commonly used in IoT scenarios to recognize/identify things, record metadata, and control distinct targets through radio waves [29]. The basic RFID system architecture contains tags and readers [30]. Tags are associated with objects for identification and readers read these tags using a close proximity communication technology. When connected to the Internet, RFID remote readers can automatically recognize, track, and monitor any object with a global tag, and in real time if needed [31]. Pateriya et al. [32] point out that vulnerable tags are subject to spying, spoofing, traffic analysis, and denial of service attacks. Unauthorized reader can access these vulnerable tags without proper access privileges. Although the tag information could potentially be protected using lightweight security mechanisms, tracking is easy to accomplish through tag replies.

User identification is currently implemented in almost all mobile platforms, using a variety of mechanisms including face recognition, fingerprints, and/or voice recognition. Surveillance systems also implement face and voice recognition using embedded cameras and microphones, respectively. An unauthorized attacker could gain full access to a surveillance camera and tamper its firmware to send the data to the legitimate server and copy the attacker. Identifying customers by authorized controllers also remains a privacy threat that leads to other threats such as profiling and utility monitoring. Surveillance cameras deployed in public settings (e.g., for video analytics and customer profiling [33, 34]) utilize public facial databases (e.g., MIT-CBCL Face Recognition Database) to track users. Such systems have become available to the public use for free like marketing platforms [35]. User identification through facial recognition has indeed become an inevitable reality and significantly hurts user privacy.

4.2. User Tracking. User tracking is primarily based on user identification, and it becomes a threat when the data collected about a certain user is maintained and used to track this user's behaviour. The most famous type of user tracking is based on location. When a user is identified, binding the location history enables tracking. Location-based services require that users share their location information. Thus, user location can be tracked without users' explicit consent and likely without their knowledge. Several technologies significantly affect user tracking such as positioning techniques, which has made great developments in recent years. Positioning techniques are typically based on Global Positioning Systems (GPS), GSM, RFID, and the Wireless LAN [36, 37]. The work done in [38] shows that average Facebook users significantly underestimate the amount of data to which they allow third-party applications access.

The evolution of such technologies provides service providers with a tool to learn about personal patterns (e.g., home location, work location, and visited places), which raises the concern of location privacy intrusion. Since the IoT market is open, user location information can be abused or sold to third parties for targeted advertisements purposes. More seriously, criminals could exploit such data to perform various types of criminal activities that risk individual's life. For example, the use of GPS to stalk customers [39–41] and, generally, the uncomfortable feeling of being observed are discussed in [42]. Even when fake identity is used, the system cannot overcome such a privacy threat with location-based services enabled [43].

4.3. Profiling. Profiling [44] refers to recording and analyzing data to characterize personal behaviour to assess or infer their personal interests in a certain domain or for discrimination purposes. Off-the-shelf data mining tools can draw a clear picture of the customer needs and easily provide a detailed customer profile. Following the rule "know your customer" [45, 46], in e-commerce, online profiling is a key tool for companies to better understand their customer needs. Profiling data is increasingly used for target advertisements, Web sites personalization, and service matching. However, profiling leads to privacy violation when used to learn a customer's political and religious views, sexual orientation, and/or medical conditions [47–49], valuable information that can be shared and sold without further consent [50–54]. The rising of Internet-connected systems and the evolution of data mining algorithms and tools significantly contributed to the emergence of big data [55]. From IoT and big data perspectives, the argument is that limiting access to private/personal data negatively impacts the accuracy of the data mining exercise. Besides this conflict of interest between privacy and profiling, we noticed that identification and tracking threats further aggravate the possibilities for profiling and increase the risks of privacy leakage by data hunting black markets.

4.4. Utility Monitoring and Controlling. This threat is directly relevant to gathering data related to customers' utility usage. Such data could be used to infer user's daily life patterns. This sensitive information represents major privacy threat if acquired through an unauthorized access. However, it becomes more serious when attackers gain privileged access to control utility usage without the user's explicit permission or knowledge. Gubbi et al. [56] categorize IoT applications

into four domains: (1) Personal and Home, (2) Enterprise, (3) Utilities, and (4) Mobile. In personal and home applications, Wi-Fi is typically used to provide high bandwidth for video streaming services and support high sampling rates for audio streaming as well as control of home appliances such as air conditioners, refrigerators, and washing machines. In Enterprise applications, IoT devices collect data from workplace environment. For example, environmental monitoring applications keep track of the number of occupants and manages the utilities within the building (e.g., HVAC, lighting). If attackers gain access to these devices, they can cause financial and personal harm to owners. Although utility companies claim that they collect data to optimize their service, the granularity at which such data is collected raise concerns. Fine granularity data may reveal private information that users do not want to share. For example, collecting water usage at high sampling rate can reveal whether customers are home or not. Data analytics tools also can show when customers take showers or use the bathroom. All these are private information that users would not feel comfortable sharing with others. For example, smart grid and smart metering [57], image processing, computer vision to support video based IoT [58], and irrigation monitoring in the agricultural industries [59]. It is highly challenging to control the disclosure of all this information from these different applications. It is also readily viable that companies could store customers' data and retain it indefinitely due to increasingly advancing storage technology with continuously decreasing prices.

The increasing evolution and adoption of IoT continue to aggravate user privacy and present new challenges on supporting infrastructure to provide more robust privacy preserving techniques. Users need to be aware of entities collecting their private data, understand how this data is shared outside their control domain, evaluate the purpose of access, estimate potential data misuse, and assess associated risks and consequences. Such requirements pose additional challenges on IoT infrastructures to provide users with safe and privacy preserving environments.

Parker Higgins [60] tweeted about the unsettling similarity of the Samsung Smart TV privacy policy, which warned consumers not to discuss sensitive topics near the device [61]. This incident led Samsung to edit its privacy policy and clarify the Smart TV's data collection practices [62]. With IoT becoming an important part of everyday life, people must pay extra attention to their privacy and systems must implement ethical practices in dealing with private data. Users should always be aware of the exact purpose of data collection and understand the spectrum of potential misuse. There must be also continuous enforcing mechanisms for access policies. The control should ultimately be placed at the users' hands to make informed decisions on how their private data is collected and shared beyond their control domain.

5. Classifications of IoT Privacy Solutions

Privacy issues in traditional Internet mostly impact connected users surfing the Internet. However, in IoT scenarios, privacy concerns may affect people who are not even using any IoT service but happen to be present in the environment. In traditional Internet services, the W3C group has defined the Platform for Privacy Preferences (P3P) [63], which provides a standard language for the description of privacy preferences and policies. P3P allows for automatic negotiation of the privacy concerning parameters based on data needed to run the service and the privacy requirements set by the user. Internet applications can implement well-established authentication procedures to capture the data flow and determine whether there are any potential privacy violations and immediately notify the user. However, in IoT settings it is far complex to precisely capture privacy violations due to the lack of well-defined control domain boundaries. Therefore, IoT environments must respect the privacy of individuals and ensure that collected personal data must be used for absolutely nothing, but the intended purpose. Lastly, collected data must be stored only until it is strictly needed.

This section discusses the proposed solutions, summarized in Table 3, to overcome privacy challenges and related security issues as follows.

(i) Authentication and authorization

(ii) Edge computing and plug-in architectures

(iii) Data anonymization

(iv) Digital forgetting and data summarization

5.1. Authentication and Authorization. Authentication in IoT scenarios is challenging due to the limitations of IoT devices. However, many researchers have proposed lightweight solutions to address these limitations and support authentication in constrained environments. Lee et al. [64] proposed simple and secure key establishment to be used in IoT networks. The authors introduce an encryption method based on XOR operations to implement a lightweight cryptography protocol. The hardware implementation of this protocol is demonstrated and can be used to establish the mutual authentication procedure in a typical RFID system for IoT applications.

Porambage et al. [65] propose PAuth Key protocol, an authentication scheme and keying mechanism suitable for resource-constrained WSNs (a.k.a. IoT), irrespective of their vendor or form factor. PAuth provides application-level end-to-end security through two phases: registration and authentication. In the registration phase, end users and edge devices obtain their cryptographic credentials. The authentication phase establishes key-based authentication using mutual communication. The protocol allows end users to authenticate with the sensing nodes directly and acquire sensor data and services. The protocol supports distributed IoT applications since the certificates are lightweight and can be handled by resource-constrained devices.

Sharaf-Dabbagh et al. [66] propose a new authentication framework for IoT environments based on device fingerprinting techniques. According to their model, each IoT device has a unique fingerprint, which can be used to communicate with the cloud infrastructure. The model provides

Table 3: Summary of privacy preserving proposed solutions in IoT environments.

Solution	Summary	References
Authentication and Authorization	(i) Lightweight authentication and key establishment mechanisms (ii) Frameworks based on device fingerprinting techniques (iii) Context-aware access control models and enforcing mechanisms	[64–68]
Edge Computing and plug in architecture	(i) Software modules on the edge to overcome privacy concerns (ii) Privacy aware systems to allow user control over data (iii) Decentralized architectures based on Personal-Cloud Butlers	[69–74]
Data Anonymizing and denaturing	(i) Data brokers and separation algorithms to offer flexibility to service providers, yet respect user-predefined access rules (ii) Generalization to mask personal data (iii) Frameworks that provide emotion analytics lifecycle to allow denaturing	[75–84]
Digital Forgetting and Data Summarization	(i) Delete encrypted data when decryption key is deleted (ii) Acquire only the strictly needed data rather than all data (iii) Apply knowledge discovery in databases and data mining technologies	[85–90]

authentication of IoT devices through a twofold approach: (1) a generative model to verify that the received messages belong to a certain object; (2) validation of the sender legitimacy to ensure that it is not a malicious object. The authors adopted the infinite Gaussian mixture model (IGMM) as a generative model if the object fingerprint follows a multivariate Gaussian distribution. The second validation method is implemented using Bhattacharyya distance to compare the clustering results from IGMM with the expected cluster shape for the device. Then, the proposed framework uses transfer learning techniques to effectively detect emulation attacks, thus, differentiating between fingerprint abnormalities resulting from environments versus attacks.

Bouij-Pasquier et al. [67] propose SmartOrBAC, a context-aware authorization model that accommodates IoT network requirements. SmartOrBAC leverages real-time context to make informed authorization decisions. The authors separate functionality into multiple layers and resource-constrained devices collaborate to perform tasks using distributed processing.

Salman et al. [68] propose an authentication scheme for heterogeneous IoT environments based on Software Defined Network (SDN). SDN controllers are used to manage security parameters by implementing a trusted certificate authority. All SDN controllers rely on a central SDN controller that translates different technology-specific identities into a single shared identity scheme based on virtual IPv6 addresses. This shared identity is then used to authenticate devices and gateways. The SDN controller authenticates gateways and gateways authenticate their associated devices. The proposed scheme is performed in three steps: (1) the gateway obtains an authentication certificate from a controller, (2) things register with the gateway, and (3) IoT devices send authentication requests to the gateway. Their analysis and experimental results show that the proposed scheme is secure against replay attack, masquerade attack, and man-in-the-middle attack.

5.2. Edge Computing and Plug-In Architectures. There is a growing adoption of the edge computing paradigm [91] in the last few years. In edge computing data processing and storage occur partially at the network edge, rather than completely in the backed. Due to the increasing trend of generating data at the edge of the network, it makes more sense to leverage edge computing to resolve concerns such as latency, device limitations, security, and more importantly user privacy [92].

Davies et al. [69] discuss the concern of data privacy in IoT networks, following Geoffrey Moore's warning [93] about the discontinuity awaiting every new technology. The authors introduce a plug-in mediator solution to overcome the privacy concerns stemming from overcentralization of IoT systems. The proposed architecture suggests deploying privacy mediators (i.e., trusted software modules) into the data distribution pipeline. A mediator runs on a cloudlet [94] to enforce the privacy policy specified by sensor/user. While developers can provide sensor drivers that convert data into common formats, customers can create privacy policies that control the mediator configuration and the sensor data routing to/from that mediator. This architecture enables the implementation of various types of data privacy controls such as deletion, denaturing, summarization, inference, anonymization, and mobility.

Langheinrich [70] presents a privacy-aware system (pawS) to overcome the privacy concerns by guaranteeing that collected data remains private. It provides data collection and processing tools that notify users of what exactly is collected. Thus, the user decides what actions can be taken. The proposed architecture adopts privacy preserving principles in ubiquitous computing [71]. The architecture encompasses four components: (1) machine-readable privacy policies to provide choice and consent, (2) policy announcement mechanisms to give notice, (3) privacy proxies to support access control, and (4) policy-based data access for protected recourses. However, proximity, negotiation, and locality are not implemented in this system. This architecture presents to

customers all available options upfront to choose from, rather than forcing them to negotiate with an automated process to get the best deal.

Bagüés et al. [72] introduce a privacy preserving framework for smart homes (Sentry@HOME). The framework adopts a user-centric approach to control the dissemination of private data according to the privacy policies defined by the user. It consists of five essential components: Sentry Registry (SR), Sentry Implementation (SI), Context Handler (CH), Sentry Manager Interface (SMI), and the Noise Module (NM). The framework embeds privacy enforcements into existing smart home infrastructure. The authors demonstrate that the smart home is a safe harbour for privacy-sensitive data and that their framework acts as a guardian sentry.

Seong et al. [73] present a decentralized architecture of PrPl, which proposes Personal-Cloud Butlers as a safe harbour for personal data indexing. A butler is configured for each user to provide fine-grain access control and storage. A similar work is presented in [74] that investigates on-device sensor abstractions for augmented reality applications to prevent private data from accidental leakage from applications having privileged access to raw sensor data.

5.3. Data Anonymization. Data anonymization is the process of removing identifiable information that may lead to personal identification so that people/objects described by such data remain anonymous [75]. The purpose of data anonymization is generally to protect user privacy. Several attempts have been made to provide anonymization, image blurring, and denaturing mechanisms for IoT applications [77, 78], especially for images and videos. Denaturing is the process of using image processing techniques to blur or alter a specific part of the image to preserve personal privacy. Data anonymization not only protects user privacy but also enables service providers to use collected data to customize the services for users. Data anonymization has three main objectives [76]: protecting the privacy of involved users, hiding any information about the network internal structure, and maintaining the anonymized traffic traces as realistic as possible to the nonanonymized packet stream.

Sliwa [79] presents a new framework for anonymized data exchange that integrates user privacy, system safety, and quality of service. The main challenge is how to design a data broker that takes only general knowledge about the required data communication and possibly unaware of the semantics, yet assures reliable and secure data exchange between partners. The author also points out the challenges of developing data separation algorithms that allow for certain flexibility to service providers, yet respect the predefined access rules (personal identity, granularity).

Berrehili and Belmekki [80] present a deep risk analysis for IoT privacy threats. The authors propose several technical and nontechnical approaches to protect user privacy in IoT scenarios. They provide a recommendation for IoT app developers to inform users about potential privacy violations resulting from private data disclosure. The authors also propose that IoT devices implement an authentication algorithm to verify the source of updated files using a cryptographic mechanism. They also suggest using anonymization techniques to mask the personal information in the data before sharing.

Shinzaki et al. [81] extend the identification-based key sharing scheme to TLS to implement mutual authentication, encrypt data communication, and provide anonymization technology for the safe disclosure of data using multiple layers of meshes on a map for the utilization of positional data. Similarly, Otgonbayar et al. [82] present a new anonymization algorithm based on the k–anonymity privacy model. The proposed algorithm uses the time-based sliding window technique to manipulate IoT streams by partitioning the stream tuples based on their description.

Wang et al. [83] introduce a scalable privacy-aware IoT architecture that enables live video analytics across many cameras by combining OpenFace [95], a high accuracy open-source face recognizer, with face tracking to maintain high accuracy and achieve full frame rate speeds. Authors also use privacy mediators to enforce user-defined privacy policies (e.g., face denaturing), yet the system maintains the original videos for possible future needs (e.g., finding an evidence from a crime scene).

Addo et al. [84] present a reference framework for protecting end user's privacy throughout the emotion analytics lifecycle. They propose Affect-Driven Personalization Lifecycle (ADPL), a model to learn the privacy preferences of end users through implementing a set of privacy rules: personalized anonymity, secure multiparty privacy preservation, encrypted data provenance, image-melding and reshaping techniques, and result aggregation.

5.4. Digital Forgetting and Data Summarization. Digital forgetting is the process of provably deleting all copies of a dataset [96], while data summarization provides a high-level data abstraction to hide details or reduce granularity. Digital forgetting and data summarization are important concepts to relieve people's anxiety around data collection. Users would feel more comfortable sharing their data knowing that collected data will be wiped out once the purpose of collection is void [85].

Data summarization is classified into the following:

(i) Temporal summarization: in which collected data is a function of time (e.g., gather sensor reading per day rather than per minute)

(ii) Spatial summarization: in which collected data is a function of location (e.g., releasing location data at the zip code level rather than raw GPS readings)

As the cost of storage decreases, the ability to store a large amount of data at low cost dramatically increases. This makes it easy for entities collecting data to store it for longer time. Hence, the need for creating efficient mechanisms that periodically delete information that is no longer needed for which it was generated arises. Therefore, IoT environments must take into consideration applying either data forgetting or summarization to protect user privacy. A few experimental solutions have been recently developed that allow users to share private data over the Internet with assurance that such

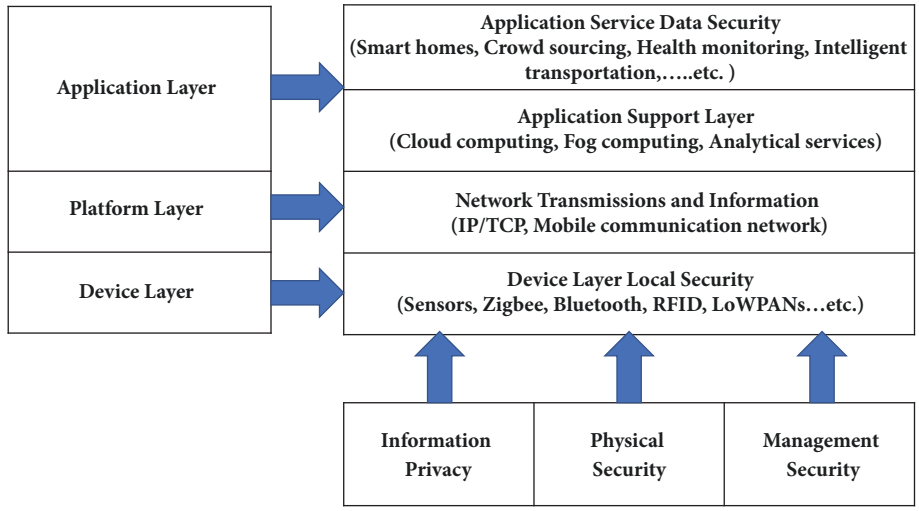

Figure 3: IoT three-layered architecture.

data will be entirely deleted after a certain period of time (e.g., drop.io and the Guest Pass features on Flickr [97]). However, porting such solutions to IoT environments is not straightforward. Therefore, several data forgetting techniques have been proposed using classical cryptography [86]. Most of these techniques assume that encrypted data is deleted when the required decryption key is deleted. Several other techniques have been developed based on distributed data storage so that data is deleted due to unavoidable social and technical processes [87].

Despite digital forgetting is an effective tool to preserve user privacy, it becomes challenging when the data size grows very large due to processing and analytics overhead [98]. Therefore, efficient data analytics techniques are required to reduce such overhead and optimize the process. To address this problem, Baraniuk [88] proposes to enforce IoT devices to acquire only important data instead of everything. Also, effective knowledge discovery in databases (KDD) and data mining techniques [89, 90] are effective solutions to summarize data collected by IoT devices, which can enhance the overall system performance and improve quality of service yet preserve user privacy. These methods are essential in IoT scenarios, in which large amounts of collected data can seriously impact the privacy of individuals and compromise the security of economic entities and government institutions.

6. Privacy Preserving IoT Environments

Applying existing Internet standards to smart devices can simplify the integration of the envisioned scenarios in the IoT contexts. However, the security mechanisms in conventional Internet protocols need to be modified or extended to preserve user privacy in IoT applications. In this section, we discuss privacy preserving at different layers of the IoT stack. We build our discussions based on a three-layer IoT stack as shown in Figure 3.

6.1. Privacy Preservation in IoT Device Layer. The IoT device layer (also known as perception layer) contains all physical resources that collect/control data (sensors and actuators). However, these resources are highly heterogeneous and resource-constrained. Such constraints pose unique challenges on applying privacy preserving techniques. Thus, IoT devices are subject to several attacks discussed in [99] including node capture, fake node, malicious data, denial of service attack (DoS), timing attack, routing threats, replay attack, side channel attack (SCA), and mass node authentication problem. Therefore, several security measures must be considered when designing this layer as follows:

(i) Access control and authentication: to prevent user privacy leaks from open and unauthorized access. Juels et al. [100] present a good solution to implement Selective RFID Jamming as an access control scheme on low-cost tags

(ii) Data encryption: to secure data exchange and guarantee safe delivery. Wang [101] presents a nonlinear key algorithm based on displaced calculation to provide data encryption. This key algorithm requires low computational power to provide high security and good data transmission rate

(iii) Secure channel using IPSec: the IPSec protocol [102] offers both authentication and encryption. Raza et al. [103] present a 6LoWPAN/IPsec extension to provide security for IoT devices. The authors demonstrate that IPSec outperforms the standard IEEE 802.15.4 link layer security in IoT environments

(iv) Cryptography technology: to offer privacy protection, confidentiality, authenticity and data integrity. Secure communication protocols include digital signatures and hash values are used to ensure data integrity

6.2. Privacy Preservation in Platform/Infrastructure Layer. The platform layer represents the classical network layer in

the OSI model [104]. This layer integrates intelligent data preprocessing to reduce resource requirements at the application layer. The network layer poses some general security problems related to data integrity and confidentiality such as unauthorized access to networks, eavesdropping, confidentiality and integrity damage, DDoS attacks, and man-in-the-middle attacks. Although existing network protocols implement highly secured measures, they are not robust enough for M2M communications in resource-constrained environments. As such, existing security mechanisms are weak/inapplicable on IoT devices and may lead to creating barriers rather than connections between different machines. Therefore, the heterogeneity of these networks makes security, interoperability, and coordination of networks becoming worse, leading to security vulnerabilities. New IoT-oriented security mechanisms must be designed from the ground up to fit IoT environments, taking into consideration the following security measures:

(i) Set up an end-to-end authentication and key agreement mechanism, PKI (Public-Key Infrastructure), WPKI for wireless, Security routing, IDS, etc.

(ii) Utilize network virtualization to reduce the network management complexity and the likelihood of improper operations.

(iii) Adopt IPv6 as a standard network layer protocol to support inherited security mechanisms [105].

6.3. Privacy Preservation in Application Layer. The application layer encompasses 2 parts: the support layer where the edge computing and analytical services run and the application service layer that provides necessary support from the IoT infrastructure. IoT applications are also highly versatile and heterogonous with varying needs, which makes it a challenge to offer a standard support. Different applications target different domains with unique data collection requirements, which may require different security measures. Therefore, the application layer security considerations/requirements differ from the previous two layers in the following sense:

(1) Nontechnical:

(a) Privacy awareness: makes users aware of private data collection, potential risks, and how to safely use IoT services and avoid private information leakage.

(b) Security management: strengthens resources, physical security information, password management, etc.

(2) Technical:

(a) Cryptography: fingerprint technology, digital watermarking, anonymous authentication, and homomorphic and threshold cryptography.

(b) Key agreements: incorporate symmetric and asymmetric cryptosystems and certification transfer technology.

7. Conclusion

The Internet of Things has the potential to change the world, just as the Internet did two decades ago. Nevertheless, any new technology faces several technical and nontechnical challenges. The highly diverse IoT application domains, resource-constrained IoT devices, and heterogeneity of both devices and platforms hinder the development of a standard IoT framework. However, privacy stands out as a critical concern that inhibits the widespread adoption IoT. The vulnerabilities of IoT devices can lead to huge security breaks and significantly hurt user privacy by exposing personal data. To promote IoT adoption and relieve user concerns, platforms, applications, and infrastructures must seriously take privacy into consideration. In this survey paper, we outline the major privacy threats in IoT environments and discuss the impact of IoT evolution on each threat. Privacy concerns such as user identification lead to a much bigger threat such as profiling. We surveyed the proposed solutions that overcome various privacy concerns and security threats in IoT environments. Most of the proposed solutions fall into one of the following categories: (1) authentication and authorization, (2) edge computing mediators, (3) data anonymization, and (4) data summarization. Consequently, several efforts were focused on providing lightweight authentication and keying establishment mechanisms, implementing frameworks based on device fingerprinting techniques, and introducing context-aware access control models.

Although the proposed solutions can relieve some of the privacy concerns in IoT scenarios, there is a clear lack of performance evaluation and assessment in real-life scenarios. Furthermore, there is a conflict between protecting user privacy and the granularity of data access needed to provide better services. This raises the challenge of how to support consumer-specific privacy preferences while maintaining the same level of service. Such a challenge could be addressed using data anonymization. The paper then points out the required measures to preserve privacy in the different layers of the IoT stack.

Our recommendation for IoT-oriented privacy preservation in IoT environments is as follows. First, take security measures into consideration at the device layer including access control and authentication, data encryption, secure channel based on IPSec, and cryptography. Second, reduce network management complexity, set up cohesive authentication mechanism, and adoption of IPv6 must be considered in the platform layer.

In conclusion, privacy preserving is a shared responsibility in which all parties much actively engage and cooperate to provide safe IoT environments yet enjoy what IoT may offer. Technology manufacturer must design IoT devices with integrated privacy and security measures. Infrastructures must implement IoT-oriented mechanisms to prevent privacy leaks and address security threats from the ground up. IoT applications must notify users of what data is collected and the purpose of collection. IoT users must take extra cautions when they authorize access to their private data and better understand the potential consequences of any associated risks resulting from any misuse of such data.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

[1] *Worldwide Internet of Things Forecast*, Sep 2017, https://www.idc.com/getdoc.jsp?containerId=IDC_P24793.

[2] Report. Gartner, *Forecast: The Internet of Things, Worldwide*, The Internet of Things, Forecast, 2017.

[3] A. Dunkels, B. Grönvall, and T. Voigt, "Contiki—a lightweight and flexible operating system for tiny networked sensors," in *Proceedings of the 29th IEEE Annual International Conference on Local Computer Networks (LCN '04)*, pp. 455–462, November 2004.

[4] E. Baccelli, O. Hahm, M. Gunes, M. Wahlisch, and T. Schmidt, "RIOT OS: Towards an OS for the Internet of Things," in *Proceedings of the 2013 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 79-80, Turin, April 2013.

[5] I. Lee and K. Lee, "The Internet of Things (IoT): Applications, investments, and challenges for enterprises," *Business Horizons*, vol. 58, no. 4, pp. 431–440, 2015.

[6] T. Rault, A. Bouabdallah, and Y. Challal, "Energy efficiency in wireless sensor networks: a top-down survey," *Computer Networks*, vol. 67, pp. 104–122, 2014.

[7] L. D. Xu, W. He, and S. Li, "Internet of things in industries: a survey," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 4, pp. 2233–2243, 2014.

[8] S. M. Riazul Islam, D. Kwak, M. Humaun Kabir, M. Hossain, and K.-S. Kwak, "The internet of things for health care: a comprehensive survey," *IEEE Access*, vol. 3, pp. 678–708, 2015.

[9] "Internet of Things (IoT): Security Analysis & Security Protocol CoAP," *International Journal of Recent Trends in Engineering and Research*, vol. 3, no. 3, pp. 417–425, 2017.

[10] Your. Proofprint, *Fridge is Full of SPAM*, 2014, [Online]., Available https://www.proofpoint.com/us/threat-insight/post/Your-Fridge-is-Full-of-SPAM.

[11] Cloud. Talkin, *Iot past and present: The history of iot, and where its headed today*, 2016, [Online]., Available http://talkincloud.com/cloud-computing/iot-past-and-present-historyiot-and-where-its-headed-today?page=2.

[12] M. Ritamaki and A. Ruhanen, "Embedded passive UHF RFID seal tag for metallic returnable transit items," in *Proceedings of the 2010 IEEE International Conference on RFID (IEEE RFID 2010)*, pp. 152–157, Orlando, FL, April 2010.

[13] J. H. Ziegeldorf, O. G. Morchon, and K. Wehrle, "Privacy in the internet of things: threats and challenges," *Security and Communication Networks*, vol. 7, no. 12, pp. 2728–2742, 2014.

[14] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial Internet of Things," in *Proceedings of the 52nd ACM/EDAC/IEEE Design Automation Conference, DAC 2015*, USA, June 2015.

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

[16] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: a review," in *Proceedings of the International Conference on Computer Science and Electronics Engineering (ICCSEE '12)*, pp. 648–651, Hangzhou, China, March 2012.

[17] M. R. Palattella, N. Accettura, X. Vilajosana et al., "Standardized protocol stack for the internet of (important) things," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 3, pp. 1389–1406, 2013.

[18] IEEE. std, *Part. 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs) Standard for Information Technology Std*, 19 IEEE std. 802.15.4 Part. 15.4, Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs) Standard for Information Technology Std. (September, 2006.

[19] T. Yu, V. Sekar, S. Seshan, Y. Agarwal, and C. Xu, "Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the Internet-of-Things," in *Proceedings of the 14th ACM Workshop on Hot Topics in Networks, HotNets-XIV 2015*, USA, November 2015.

[20] Z. Durumeric, J. Kasten, D. Adrian et al., "The matter of heartbleed," in *Proceedings of the 2014 ACM Internet Measurement Conference, IMC 2014*, pp. 475–488, Canada, November 2014.

[21] Shodan. March, *Devices Vulnerable to Heartbleed [Online]. Available*, 2016, https://www.shodan.io/report/89bnfUyJ.

[22] T. Heer, O. Garcia-Morchon, R. Hummen, S. L. Keoh, S. S. Kumar, and K. Wehrle, "Security challenges in the IP-based Internet of Things," *Wireless Personal Communications*, vol. 61, no. 3, pp. 527–542, 2011.

[23] G. O. Yee, *Privacy Protection Measures and Technologies in Business Organizations*, IGI Global, 2012.

[24] https://www.eia.gov/.

[25] A. Molina-Markham, P. Shenoy, K. Fu, E. Cecchet, and D. Irwin, "Private memoirs of a smart meter," in *Proceedings of the 2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Buildings, BuildSys'10*, pp. 61–66, Switzerland, November 2010.

[26] U. Feige, A. Fiat, and A. Shamir, "Zero-knowledge proofs of identity," *Journal of Cryptology*, vol. 1, no. 2, pp. 77–94, 1988.

[27] T. Datta, N. Apthorpe, and N. Feamster, "A Developer-Friendly Library for Smart Home IoT Privacy-Preserving Traffic Obfuscation," in *Proceedings of the the 2018 Workshop*, pp. 43–48, Budapest, Hungary, August 2018.

[28] K. Yang, K. Zhang, J. Ren, and X. Shen, "Security and privacy in mobile crowdsourcing networks: challenges and opportunities," *IEEE Communications Magazine*, vol. 53, no. 8, pp. 75–81, August 2015.

[29] X. Jia, Q. Feng, and C. Ma, "An efficient anti-collision protocol for RFID tag identification," *IEEE Communications Letters*, vol. 14, no. 11, pp. 1014–1016, 2010.

[30] K. Finkenzeller, "RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and near-Field Communication," *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and near-Field Communication*, 2010.

[31] G. T. Huang, "10 emerging technologies that will change your world," *IEEE Engineering Management Review*, vol. 32, no. 2, pp. 20-20, 2004.

[32] R. K. Pateriya and S. Sharma, "The evolution of RFID security and privacy: A research survey," in *Proceedings of the 2011 International Conference on Communication Systems and Network Technologies, CSNT 2011*, pp. 115–119, India, June 2011.

[33] X. Liu, N. Krahnstoever, T. Yu, and P. Tu, "What are customers looking at?" in *Proceedings of the 2007 IEEE Conference on Advanced Video and Signal Based Surveillance, AVSS 2007*, pp. 405–410, UK, September 2007.

[34] A. W. Senior, L. Brown, A. Hampapur et al., "Video analytics for retail," in *Proceedings of the 2007 IEEE Conference on Advanced Video and Signal Based Surveillance, AVSS 2007*, pp. 423–428, UK, September 2007.

[35] *Handbook of Face Recognition*, Springer-Verlag, New York, 2005.

[36] *Pro PayPal E-Commerce*, Apress, Berkeley, CA, 2007.

[37] J. Wrrior, E. McHenry, and K. McGee, "They know where you are," *IEEE Spectrum*, vol. 40, no. 7, pp. 20–25, 2003.

[38] J. Golbeck and M. L. Mauriello, "User perception of Facebook app data access: A comparison of methods and privacy concerns," *Future Internet*, vol. 8, no. 2, 2016.

[39] J. Voelcker, "Stalked by satellite—an alarming rise in GPS-enabled harassment," *IEEE Spectrum*, vol. 43, no. 7, pp. 15-16, 2006.

[40] M. Z. Newman, "Crazy Ex-Girlfriend," *Film Criticism*, vol. 40, no. 3, 2016.

[41] Cop stalked ex-wife before killing her, https://www.usatoday.com/story/news/nation//07/29/cop-stalked-ex-wife//.

[42] C. Chow and M. F. Mokbel, "Privacy in location-based services," *SIGSPATIAL Special*, vol. 1, no. 2, pp. 23–27, 2009.

[43] E. Toch, Y. Wang, and L. F. Cranor, "Personalization and privacy: A survey of privacy risks and remedies in personalization-based systems," *User Modeling and User-Adapted Interaction*, vol. 22, no. 1-2, pp. 203–220, 2012.

[44] M. Hildebrandt, "Defining profiling: A new type of knowledge?" *Profiling the European Citizen: Cross-Disciplinary Perspectives*, pp. 17–45, 2008.

[45] Patrick. Thibodeau, Online Profiling, [Online], https://www.computerworld.com/article/2597220/retail-it/online-profiling.html.

[46] A. Odlyzko, "Privacy, economics, and price discrimination on the Internet," in *Proceedings of the the 5th international conference*, pp. 355–366, Pittsburgh, Pennsylvania, September 2003.

[47] *Profiling and Targeting - Behavioral Advertisers Beware!*, [Online], URL https://www.ecommercetimes.com/story/73966.html.

[48] G. L. Orgill, G. W. Romney, M. G. Bailey, and P. M. Orgill, "The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems," in *Proceedings of the the 5th conference*, p. 177, Salt Lake City, UT, USA, October 2004.

[49] G. T. Marx, "The surveillance society: the threat of 1984-style techniques. in. The Futurist," in *June 21-6*, p. 21, The surveillance society, the threat of 1984-style techniques. in. The Futurist, 1985.

[50] A. Vedder, "KDD: The challenge to individualism," *Ethics and Information Technology*, vol. 1, no. 4, pp. 275–281, 1999.

[51] D. Lyon, *Surveillance as Social Sorting*, Routledge, 2005.

[52] B. Custers, "Effects of unreliable group profiling by means of data mining," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Preface*, vol. 2843, pp. 291–296, 2003.

[53] M. Hildebrandt and S. Gutwirth, *Profiling the European Citizen*, Springer Netherlands, Dordrecht, 2008.

[54] J. Menn, "Social networks scan for sexual predators, with uneven results," in *Reuters. [Online. Last accessed*, pp. 2013-02, 2012, [Online. Last accessed 2013-02-07] http://reut.rs/Nnejb7.

[55] S. John Walker, "Big Data: A Revolution That Will Transform How We Live, Work, and Think," *International Journal of Advertising*, vol. 33, no. 1, pp. 181–183, 2015.

[56] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): a vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[57] M. Yun and B. Yuxin, "Research on the architecture and key technology of Internet of Things (IoT) applied on smart grid," in *Proceedings of the International Conference on Advances in Energy Engineering (ICAEE '10)*, pp. 69–72, June 2010.

[58] I. F. Akyildiz, T. Melodia, and K. R. Chowdhury, "A survey on wireless multimedia sensor networks," *Computer Networks*, vol. 51, no. 4, pp. 921–960, 2007.

[59] L. Zhao, S. Yin, L. Liu, Z. Zhang, and S. Wei, "A crop monitoring system based on wireless sensor network," in *Proceedings of the 2011 2nd International Conference on Challenges in Environmental Science and Computer Engineering, CESCE 2011*, pp. 558–565, China, December 2011.

[60] Smart. Samsung's, TV privacy policy sounds like an Orwellian nightmare [online], https://www.theverge.com//2/8//samsungs-smart-tv-privacy-policy-george-orwell.

[61] https://epic.org/privacy/internet/ftc/EPIC-Letter-FTC-AG-Always-On.pdf.

[62] Y.-A. de Montjoye, *Computational PRIvacy: Towards PRIvacy-Conscientious Uses of Metadata*, ProQuest LLC, Ann Arbor, MI, 2015.

[63] J. Reagle and L. F. Cranor, "The platform for privacy preferences," *Communications of the ACM*, vol. 42, no. 2, pp. 48–55.

[64] J.-Y. Lee, W.-C. Lin, and Y.-H. Huang, "A lightweight authentication protocol for Internet of Things," in *Proceedings of the 3rd International Symposium on Next-Generation Electronics, ISNE 2014*, Taiwan, May 2014.

[65] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, "Pauthkey: a pervasive authentication protocol and key establishment scheme for wireless sensor networks in distributed IoT applications," *International Journal of Distributed Sensor Networks*, vol. 2014, Article ID 357430, 14 pages, 2014.

[66] Y. Sharaf-Dabbagh and W. Saad, "On the authentication of devices in the Internet of things," in *Proceedings of the 17th International Symposium on a World of Wireless, Mobile and Multimedia Networks, WoWMoM 2016*, Portugal, June 2016.

[67] I. Bouij-Pasquier, A. Ait Ouahman, A. Abou El Kalam, and M. Ouabiba De Montfort, "SmartOrBAC security and privacy in the Internet of Things," in *Proceedings of the 12th IEEE/ACS International Conference of Computer Systems and Applications, AICCSA 2015*, November 2015.

[68] O. Salman, S. Abdallah, I. H. Elhajj, A. Chehab, and A. Kayssi, "Identity-based authentication scheme for the Internet of Things," in *Proceedings of the 2016 IEEE Symposium on Computers and Communication, ISCC 2016*, pp. 1109–1111, Italy, July 2016.

[69] N. Davies, N. Taft, M. Satyanarayanan, S. Clinch, and B. Amos, "Privacy mediators: Helping IoT cross the chasm," in *Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications, HotMobile 2016*, pp. 39–44, USA, February 2016.

[70] M. Langheinrich, "A Privacy Awareness System for Ubiquitous Computing Environments," in *UbiComp 2002: Ubiquitous Computing*, vol. 2498 of *Lecture Notes in Computer Science*, pp. 237–245, Springer Berlin Heidelberg, Berlin, Heidelberg, 2002.

[71] M. Langheinrich, "Privacy by design-principles of privacy-aware ubiquitous systems," in *Proceedings of the Ubicomp 2001: Ubiquitous Computing*, Lecture Notes in Computer Science, pp. 273–291, Springer, Berlin, Germany, 2001.

[72] S. A. Bagüés, A. Zeidler, F. Valdivielso, and I. R. Matias, "Sentry@Home - Leveraging the smart home for privacy in pervasive computing," *International Journal of Smart Home*, vol. 1, no. 2, pp. 129–146, 2007.

[73] S.-W. Seong, J. Seo, M. Nasielski et al., "PrPl: A decentralized social networking infrastructure," in *Proceedings of the 1st ACM Workshop on Mobile Cloud Computing and Services: Social Networks and Beyond, MCS'10, Co-located with ACM MobiSys 2010*, USA, June 2010.

[74] J. Vilk, D. Molnar, B. Livshits et al., "SurroundWeb: Mitigating Privacy Concerns in a 3D Web Browser," in *Proceedings of the 2015 IEEE Symposium on Security and Privacy (SP)*, pp. 431–446, San Jose, CA, May 2015.

[75] B. Zhou, J. Pei, and W. Luk, "A brief survey on anonymization techniques for privacy preserving publishing of social network data," *ACM SIGKDD Explorations Newsletter*, vol. 10, no. 2, p. 12, 2008.

[76] D. Koukis, S. Antonatos, D. Antoniades, E. P. Markatos, and P. Trimintzios, "A generic anonymization framework for network traffic," in *Proceedings of the 2006 IEEE International Conference on Communications, ICC 2006*, pp. 2302–2309, Turkey, July 2006.

[77] M. K. Reiter and A. D. Rubin, "Crowds: anonymity for Web transactions," *ACM Transactions on Information and System Security*, vol. 1, no. 1, pp. 66–92.

[78] *Benezit Dictionary of Artists*, Oxford University Press, 2011.

[79] J. Sliwa, "A generalized framework for multi-party data exchange for IoT systems," in *Proceedings of the 30th IEEE International Conference on Advanced Information Networking and Applications Workshops, WAINA 2016*, pp. 193–198, Switzerland, March 2016.

[80] F. Z. Berrehili and A. Belmekki, "Privacy Preservation in the Internet of Things," in *Advances in Ubiquitous Networking 2*, vol. 397 of *Lecture Notes in Electrical Engineering*, pp. 163–175, Springer Singapore, Singapore, 2017.

[81] T. Shinzaki, I. Morikawa, Y. Yamaoka, and Y. Sakemi, "IoT security for utilization of big data: Mutual authentication technology and anonymization technology for positional data," *Fujitsu scientific & technical journal*, vol. 52, no. 4, pp. 52–60, 2016.

[82] A. Otgonbayar, Z. Pervez, and K. Dahal, "Toward Anonymizing IoT Data Streams via Partitioning," in *Proceedings of the 13th IEEE International Conference on Mobile Ad Hoc and Sensor Systems, MASS 2016*, pp. 331–336, Brazil, October 2016.

[83] J. Wang, B. Amos, A. Das, P. Pillai, N. Sadeh, and M. Satyanarayanan, "A scalable and privacy-aware IoT service for live video analytics," in *Proceedings of the 8th ACM Multimedia Systems Conference, MMSys 2017*, pp. 38–49, Taiwan, June 2017.

[84] I. D. Addo, P. Madiraju, S. I. Ahamed, and W. C. Chu, "Privacy Preservation in Affect-Driven Personalization," in *Proceedings of the 2016 IEEE 40th Annual Computer Software and Applications Conference, COMPSAC 2016*, pp. 400–405, USA, June 2016.

[85] C. Thompson, "25 Ideas for 2010: Digital Forgetting," *25 Ideas for 2010: Digital Forgetting*, November 2009.

[86] D. Boneh and R. J. Lipton, "A revocable backup system," *in USENIX Security*, pp. 91–96, 1996.

[87] S. Diesburg, C. Meyers, M. Stanovich et al., "TrueErase," in *Proceedings of the the 28th Annual Computer Security Applications Conference*, p. 439, Orlando, Florida, December 2012.

[88] R. G. Baraniuk, "More is less: Signal processing and the data deluge," *Science*, vol. 331, no. 6018, pp. 717–719, 2011.

[89] V. Cantoni, L. Lombardi, and P. Lombardi, "Challenges for data mining in distributed sensor networks," in *Proceedings of the 18th International Conference on Pattern Recognition, ICPR 2006*, pp. 1000–1007, China, August 2006.

[90] T. Keller, F. Thiesse, J. Kungl, and E. Fleisch, "Using low-level reader data to detect false-positive RFID tag reads," in *Proceedings of the Internet of Things (IOT '10)*, vol. 7, pp. 1–8, IEEE, Tokyo, Japan, December 2010.

[91] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: vision and challenges," *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 637–646, 2016.

[92] W. Shi and S. Dustdar, "The Promise of Edge Computing," *The Computer Journal*, vol. 49, no. 5, pp. 78–81, 2016.

[93] G. Moore, *Crossing the Chasm*, Harpercollins, 1991.

[94] M. Satyanarayanan, P. Bahl, R. Cáceres, and N. Davies, "The case for VM-based cloudlets in mobile computing," *IEEE Pervasive Computing*, vol. 8, no. 4, pp. 14–23, 2009.

[95] T. Baltrusaitis, P. Robinson, and L.-P. Morency, "OpenFace: An open source facial behavior analysis toolkit," in *Proceedings of the IEEE Winter Conference on Applications of Computer Vision, WACV 2016*, pp. 1–10, March 2016.

[96] Z. N. Peterson, R. C. Burns, J. Herring, A. Stubblefield, A. D. Rubin, and A. Stubblefield, "Secure deletion for a versioning file system," *in File and Storage Technologies (FAST*, vol. 5, p. 11, 2005.

[97] N. Proferes, "Delete: The Virtue of Forgetting in the Digital Age. Viktor Mayer-Schönberger. Princeton, NJ: Princeton University Press, 2009.," *The Journal of Popular Culture*, vol. 45, no. 1, pp. 226–228, 2012.

[98] D. Reed, J. Larus, and D. Gannon, "Imagining the future: thoughts on computing," *The Computer Journal*, vol. 45, no. 1, pp. 25–30, 2012.

[99] K. Zhao and L. Ge, "A survey on the internet of things security," in *Proceedings of the 9th International Conference on Computational Intelligence and Security, CIS 2013*, pp. 663–667, December 2013.

[100] A. Juels, R. L. Rivest, and M. Szydlo, "The blocker tag: Selective blocking of RFID tags for consumer privacy," in *Proceedings of the 10th ACM Conference on Computer and Communications Security, CCS 2003*, pp. 103–111, USA, October 2003.

[101] X. Yi, Y. Liang, E. Huerta-Sanchez et al., "Sequencing of 50 human exomes reveals adaptation to high altitude," *Science*, vol. 329, no. 5987, pp. 75–78, 2010.

[102] S. Kent and K. Seo, "Security Architecture for the Internet Protocol," RFC Editor RFC4301, 2005.

[103] S. Raza, S. Duquennoy, J. Höglund, U. Roedig, and T. Voigt, "Secure communication for the Internet of Things-a comparison of link-layer security and IPsec for 6LoWPAN," *Security and Communication Networks*, vol. 7, no. 12, pp. 2654–2668, 2014.

[104] H. Zimmermann, "OSI reference model—the ISO model of architecture for open systems interconnection," *IEEE Transactions on Communications*, vol. 28, no. 4, pp. 425–432, 1980.

[105] S. Liang, Y. Zhang, and G. Jian, *Development Trend of IPv6-based Information Security Products in Network Layer of IOT [J]. Netinfo Security 8*, 018, 2012.