A Privacy-Enhancing Framework for Internet of Things Services

Lukas Malina[1]* , Gautam Srivastava[2,3], Petr Dzurenda[1], Jan Hajny[1], and Sara Ricci[1]

[1] Department of Telecommunications, Brno University of Technology, Brno, Czech Republic; E-mail: {malina, dzurenda, hajny, ricci}@feec.vutbr.cz

[2] Department of Mathematics and Computer Science, Brandon University, 270 18th Street, Brandon, Canada, R7A 6A9; srivastavag@brandonu.ca

[3] Research Center for Interneural Computing, China Medical University, Taichung 40402, Taiwan, Republic of China

Keywords: Authentication; Cryptography; Evaluation; Identification; Internet of Things; Privacy; Privacy-Enhancing Technologies; Security; Safety.

Abstract

The world has seen an influx of connected devices through both smart devices and smart cities, paving the path forward for the Internet of Things (IoT). These emerging intelligent infrastructures and applications based on IoT can be beneficial to users only if essential private and secure features are assured. However, with constrained devices being the norm in IoT, security and privacy are often minimized. In this paper, we first categorize various existing privacy-enhancing technologies (PETs) and assessment of their suitability for privacy-requiring services within IoT. We also categorize potential privacy risks, threats, and leakages related to various IoT use cases. Furthermore, we propose a simple novel privacy-preserving framework based on a set of suitable privacy-enhancing technologies in order to maintain security and privacy within IoT services. Our study[4] can serve as a baseline of privacy-by-design strategies applicable to IoT based services, with a particular focus on smart things, such as safety equipment.

1 Introduction

Emerging Intelligent Infrastructures (II) that interconnect various IoT applications and services are meant to provide convenience to people, open new benefits to society, and benefit our environment. There are many IoT applications and use cases that are either already implemented or are in varying research stages heading towards potential implementation. The general overview of IoT environments and applicable scenarios are depicted in Figure 1.

[4] The final authenticated publication is available online at `https://doi.org/10.1007/978-3-030-36938-5_5`

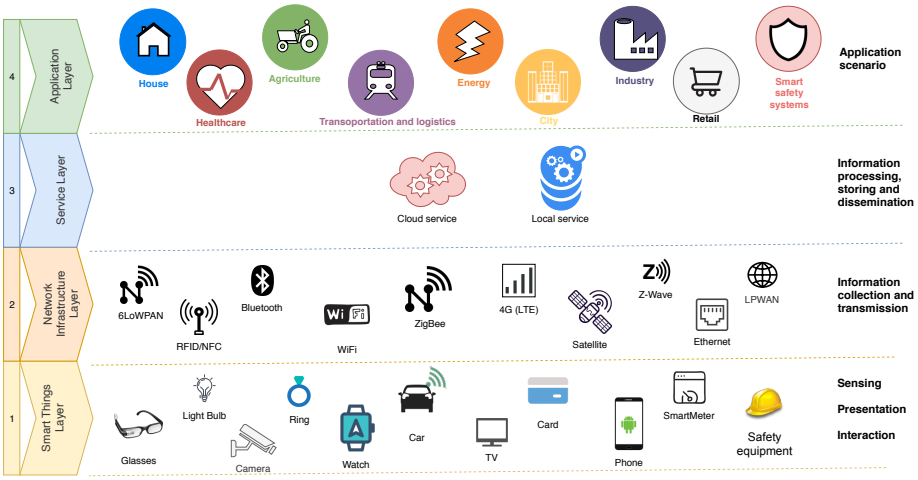

Fig. 1. The IoT environment and application areas.

Nevertheless, connected objects, sensors and digital systems around peoples lives form a large intelligent network that can serve as a medium for the leakage of personal data [61, 27, 63]. It is essential during the design and application stages of intelligent networks to include privacy protection into incoming infrastructures and IoT applications. Engineers, practitioners, and researchers can develop various privacy protection principles, technologies or Privacy by Design (PbD) strategies. PbD is a term for a multifaceted concept which involves various technological and organizational components, implementing privacy, and data protection principles. In [18], Hoepman proposes eight privacy design strategies, divided into 2 categories, namely data-oriented (1-4) and process-oriented (5-8). The strategies are briefly described as follows:

1. **Minimize**: processed personal data should be constrained to the minimal amount.
2. **Hide**: personal data and their interrelationships (linkability) should be protected or not public.
3. **Separate**: personal data should be processed in a distributed way.
4. **Aggregate** (Abstract): limit as much as possible the detail in which personal data is processed, aggregating data in the highest level.
5. **Inform**: data subjects should be informed whenever their personal data is processed.
6. **Control**: data subjects should be provided control over the processing of their personal data.
7. **Enforce**: processing personal data should be committed in a privacy-friendly way, and should be adequately enforced.
8. **Demonstrate**: the system should able to demonstrate compliance with the privacy policy and any applicable legal requirements.

Many PbD strategies can be solved by privacy protection techniques called Privacy-Enhancing Technologies (PETs). PETs are based on the principles of data minimization, anonymization, pseudonymization, and data protection that allow users to protect their privacy and their personally identifiable information (PII).

The European Union Agency for Network and Information Security (ENISA) has been active in PETs for many years by collaborating closely with privacy experts from academia and industry. ENISA defines PETs as the broader range of technologies that are designed for supporting privacy and data protection. The ENISA report given in [8] provides a fundamental inventory of the existing approaches and privacy design strategies and the technical building blocks of various degree of maturity from research and development in general ICT. The report [8] distinguishes the following basic privacy techniques:

- **Authentication** (e.g. privacy features of authentication protocols);
- **Attribute-based credentials**;
- **Secure private communications**;
- **Communications anonymity and pseudonymity**;
- **Privacy in databases**:
  - Respondent privacy: statistical disclosure control;
  - Owner privacy: privacy-preserving data mining;
  - User privacy: private information retrieval;
- **Storage privacy**;
- **Privacy-preserving computations**;
- **Transparency-enhancing techniques**;
- **Intervenability-enhancing techniques**.

In this paper, we focus on privacy-preserving techniques that can be deployed in IoT based services.

1.1 Privacy in Standards and Regulations

Privacy protection is already an important part of EU regulations and international standards. In 2011, the ISO organization released the ISO/IEC 29100:2011 Privacy Framework Standard that aims at the protection of PII from the beginning of data collection, data usage, data storage to final data destruction. The standard presents 11 principles:

1. consent and choice
2. purpose legitimacy and specification
3. collection limitation
4. data minimization
5. use, retention, and disclosure limitation
6. accuracy and quality
7. openness, transparency, and notice
8. individual participation and access
9. accountability
10. information security

11. privacy compliance

The general data protection regulation (GDPR) replaced the Data Protection Directive 95/46/EC in 2018 [57]. The GDPR covers most basic data security and privacy principles by Article 5 that includes lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability. In addition, the GDPR is stricter in various privacy aspects such as consent, right to be forgotten and privacy (and data protection) by design and by default that is mentioned in Article 25. Hence, privacy-preserving IoT applications and services are required also by the above-mentioned regulations.

1.2 Privacy in IoT Applications and Communication Model

In general, a common IoT communication model consists of several entities such as users, service providers, and third parties. It is also defined by several processes, such as data sensing, interaction, collection, and presentation. Ziegeldorf *et al.* present an IoT model with 4 different IoT entities [64]. Those entities are smart things (IoT sensors, actuators), services (backends), subjects (humans who receive data and/or produce/send data), and infrastructures (including network sub-entities based communication technologies). They also introduce 5 different IoT data flows: interaction, presentation, collection, dissemination and processing.

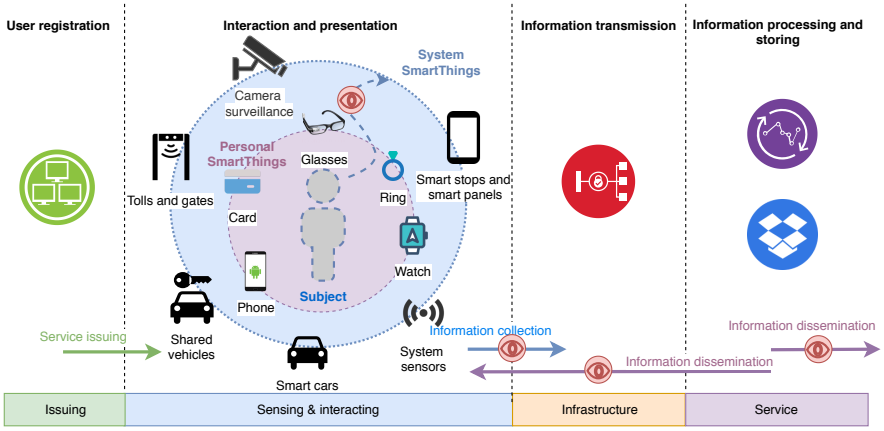

Fig. 2. The IoT communication model and privacy breaches.

Figure 2 depicts our view of an IoT model and potential privacy breaches that are marked with eye icons. The human interaction with proximity and vicinity IoT smart things (sensors, interfaces) may lead to several privacy threats and

leakages that have to be mitigated. The list of privacy issues is presented in detail in Section 4.

In this paper, we aim at privacy-required IoT applications and privacy issues in IoT. We also provide an assessment of technical-based PETs in various IoT applications. Based on the results of our categorization and assessment, we propose a novel general framework that should address potential privacy leakages and threats within data processes in various IoT scenarios. Our framework enhances traditional privacy-preserving models (e.g. Hoepman's eight privacy design strategies [18]) by concrete steps and privacy-preserving technical countermeasures suited for private and secure IoT services.

The rest of the paper is organized as follows. In Section 2 we describe the state-of-the-art. We follow this in Section 3 by exploring specific use cases of IoT where users have or may experience privacy issues. Section 4 presents privacy issues in IoT. Next, in Section 5 we deal with the categorization and assessment of PETs in IoT. Section 6 presents our proposal of a general privacy-preserving framework for IoT. Lastly, we give some concluding remarks in Section 7.

2 State of the Art

There are plenty of interesting studies and survey papers focusing on security and privacy in IoT [42, 48, 29, 41, 23]. Furthermore, there are surveys and study papers that focus solely on privacy in IoT. Some examples are given in [36, 25, 44, 6, 45, 22].

Seliem *et al.* review existing research and propose solutions to rising privacy concerns from a multiple viewpoint to identify the risks and mitigations in [44]. The authors provide an evaluation of privacy issues and concerns in IoT systems due to resource constraints. They also describe IoT solutions that embrace a variety of privacy concerns such as identification, tracking, monitoring, and profiling. Sen *et al.* deal with differences between privacy and security in [45]. The authors present 11 general approaches and techniques that are being used to fulfill privacy requirements. Nevertheless, their analysis and classification models are not very deep. Vasilomanolakis *et al.* provide comparative analysis of four IoT architectures. Those are IoT-A, BeTaaS, OpenIoT, and IoT@Work [55]. The authors compare the general security requirements and four privacy features (data privacy, anonymity, pseudonymity, unlinkability) of the IoT architectures. The paper concludes stating that IoT-A and IoT@Work provide some privacy protection but privacy and identity management requirements should be balanced. Furthermore, Li *et al.* review the state-of-the-art principles of privacy laws as well as the architectures for IoT and the representative PETs [22]. The authors demonstrate how privacy legislation maps to privacy principles which in turn drive the design of privacy-enhancing technologies. The authors consider 4 layers such as the perception layer (data sensing), networking layer (data transaction), middleware layer (data storage and processing) and application layer (data presentation and usage), and they classify and analyze PETs by these layers. In [6], Cha *et al.* survey 120 papers focusing on the solutions of PETs in IoT. Authors classify PETs in IoT into 7 research domains:

- Control Over Data
- Enforcement
- Anonymization or Pseudonymization

– Personal Data Protection

- Anonymous Authorization
- Partial Data Disclosure
- Holistic Privacy Preservation

Furthermore, the authors conduct 15 privacy principles from GDPR and ISO/IEC 29100:2011, and link the principles with PETs papers and present some future directions of advanced technologies. The classification of 120 privacy-oriented IoT papers shows that 28% of papers are dedicated to building and home automation, 13% for e-healthcare, 13% for smart cities, 9% for wearables, 8% for automotive, 2% smart manufacturing and 27% are general oriented. In our study, we categorize and present concrete privacy-required IoT applications in Section 3.

The above noted surveys provide comprehensive literature reviews about the PETs including several classifications but there are a lack of basic guidelines for a privacy-by-design implementation of privacy-requiring IoT applications and concrete PETs recommendations.

3 Privacy-Requiring IoT Applications and Use Cases

With the new conveniences promised by IoT comes new privacy and security vulnerabilities. In an area where often times the devices involved are constrained and as such do not have the capabilities of running high powered security protection, we see definitive vulnerabilities. In this section, we will explore some specific use cases of IoT where users have or may experience privacy issues in no particular order.

In late 2015, two security researchers were able to show that over $68,000$ medical device systems were exposed online, and that $12,000$ of them belonged to one healthcare organization [35]. The major concern with this discovery was that these devices were connected to the Internet through computers running very old versions of Windows XP, a version of the OS which is known to have lots of exploitable vulnerabilities. This version of Windows although dated is still to this day part of many legacy systems worldwide, adding to the future privacy threats to IoT devices connected to such systems. These devices were discovered by using Shodan, a search engine that can find IoT devices online that are connected to the internet. These are easy to hack via brute-force attacks and using hard-coded logins. During their research, the two experts found anesthesia equipment, cardiology devices, nuclear medical systems, infusion systems, pacemakers, magnetic resonance imaging (MRI) scanners, and other devices all via simple Shodan queries. Although not yet ever reported, there is a chance that hackers gaining access to medical devices may change settings to these devices which could cause physical harm to someone connected to such a device.

For smart home IoT, one well documented attack is the Fingerprint and Timing based Snooping (FATS) attack presented by Srinivasan *et al.* in [50]. The FATS attack involves activity detection, room classification, sensor classification, and activity recognition from Wi-Fi traffic metadata from a sensor network deployed in the home the precursor to todays smart home IoT devices. The FATS attack relies on wireless network traffic instead of observations from a last-mile Internet service provider or other adversary located on a Wide Area Network (WAN). The FATS attack demonstrates that traffic analysis attacks in the style of FATS are as effective for the current generation of consumer IoT devices as they were for sensor networks ten years ago.

In another significant real-world attack, a recent article in Forbes magazine highlighted research by Noam Rotem and Ran Locar at vpnMentor, who exposed a Chinese company called Orvibo, which runs an IoT management platform. They showed that their database was easily accessible through direct connection to it, exposing openly user logs which contained 2 billion records including user passwords, account reset codes, payment information and even some "smart" camera recorded conversations. Below is a list of data that was available through this ground-breaking breach.

- Email addresses
- Passwords
- Account reset codes
- Precise Geolocation
- IP Address
- Username (ID)
- Family name

This specific breach pinpoints the type of data can be available through unsecured IoT devices or networks.

Consider another IoT use case involving assisted living, were we consider senior citizens who appreciate living independently as summarized in [16]. In this scenario, a number of unobtrusive sensors screen their vital signs and deliver information to the cloud for fast access by family members and third parties such as doctors, and health care providers. There are two levels of privacy issues here, one dealing with senior citizen medical information and the other with their personal data. Combining IoT devices for monitoring vitals and storage mechanisms like cloud storage can present a new domain of issues trying to integrate constrained devices (IoT) with the unconstrained (cloud storage).

Important social challenges stem from the necessity to adapt Smart City services to the specific characteristics of every user [60]. A service deployed in a Smart City may have many configurations options, depending on user expectations and preferences; the knowledge of these preferences usually means the success or failure of a service. In order to adapt a service to the specific users preferences, it is necessary to know them, and this is basically done based on a characterization of that specific user. Nevertheless, a complete characterization of user preferences and behavior can be considered as a personal threat, so the

great societal challenge for this, and for any service requiring user characterization, is to assure users privacy and security. Thus, in order to achieve user consent, trust in, and acceptance of Smart Cities, integration of security and privacy preserving mechanisms must be a key concern of future research. The overall priority must be to establish user confidence in the upcoming technologies, as otherwise users will hesitate to accept the services provided by Smart Cities.

In the near future autonomous vehicles will be commonplace [59, 21]. In the meantime, the development of Internet of Vehicles (IoV) is ongoing where a myriad of sensors, devices and controllers are attached to vehicles in an effort to allow for autonomous control. It is quite significant to design a privacy mechanism which ensures that collection of IoV Big Data is trusted and not tampered with. There is a huge risk of fraudulent messages injected by a malicious vehicle that could easily endanger the whole traffic system(s) or could potentially employ the entire network to pursue any dangerous activity for its own wicked benefits.

Finally, in [49], Solanas *et al.* discuss the notions of Smart Health (s-Health), as the synergy between mobile health and smart cities. Although s-Health might help to mitigate many health related issues, its ability to gather unprecedented amounts of information could endanger the privacy of citizens. In the context of s-Health, the information gathered is often rather personal. From the data, it would be possible to infer citizens habits, their social status, and even their religion. All these variables are very sensitive, and when they are combined with health information, the result is even more delicate. This s-Health scenarios are also very related to smart safety systems where protective equipment (such as helmets, glasses or hazmat suites) is being monitored and traced.

We summarize our findings listing areas of IoT, some concrete applications, and the privacy concerns in Table 1. The privacy concerns used match the list from [13], where Finn *et al.* identify 7 privacy concerns, defined as follows:

- **Privacy of person**: encompasses the right to keep body functions and body characteristics private.
- **Privacy of behaviour and action**: this concept includes sensitive issues such as sexual preferences and habits, political activities and religious practices.
- **Privacy of communication**: aims to avoid the interception of communications, including mail interception, the use of bugs, directional microphones, telephone or wireless communication interception or recording and access to e-mail messages.
- **Privacy of data and image**: includes concerns about making sure that individuals data is not automatically available.
- **Privacy of thoughts and feelings**. People have a right not to share their thoughts or feelings.
- **Privacy of location and space**: individuals have the right to move about in public or semi-public space without being identified.
- **Privacy of association**: says that people have a right to associate with whomever they wish, without being monitored.

Table 1. IoT Areas with the Example of Applications and Privacy Concerns [13]

IoT Area	Application	Privacy Concerns
Healthcare IoT	Geniatech, Cycore	Data, Person
Internet of Underwater Things	WFS Tech	Communication
Smart Home	Orvibo	Data, Location
Smart Cities	Cisco	Communication, Location Data
IoT Blockchain Implementations	Helium	Personal, Data
Internet of Vehicles	RideLogic	Action, Image

4 Categorization of Privacy Issues: Threats, Leakages and Attacks in an IoT Environment

In this section, we categorize privacy issues and present brief descriptions, potential prevention approaches and compromised IoT areas. Security attacks and privacy threats in IoT have been analyzed in various studies [33, 64, 2, 6]. Lopez *et al.* detect 3 IoT privacy problems: user privacy, content privacy and context privacy [25]. Furthermore, there have been seven privacy threat categories for IoT given in [64, 6]. Our analysis presents 12 privacy issues divided into 3 classes:

- privacy **threats**: this class represents the weaknesses and flaws of IoT services and systems that could be misused by other system entities and/or lead to leakages and attacks,
- privacy **leakages**: this class represents more serious problems and flaws that can directly breach user privacy and/or can be misused by passive and active attackers,
- privacy **attacks**: this class represents issues that are intentionally performed by passive and active attackers in order to break user privacy and misuse the observed information for criminal activities.

We categorize general privacy protection and prevention approaches as follows:

- *Data minimization*: limiting data collection to only necessary information.
- *Data anonymization*: encrypting, modifying or removing personal information in such a way that the data can no longer be used to identify a natural person.
- *Data security*: the process of protecting data from unauthorized access and data corruption.
- *Data control*: monitoring and controlling the data by defining policies.
- *Identity management*: policies and technologies for ensuring that the proper users have access to technology resources.
- *Secure communication*: communication protocol that allow people sharing information with the appropriate confidentiality, source authentication, and data integrity protection.

- *User awareness/informed consent transparency*: users give their consents about data usage and they are aware which data are processed.

In Table 2, we describe privacy issues, general prevention approaches and link the issues with target IoT area and services. To be noted, that some more complex attacks can be performed by the combination of several privacy leakages and threats.

5 Categorization of Privacy-Enhancing Technologies for Internet of Things

In this section, we present and categorize privacy-enhancing technologies. We focus on `PETs` that can be

- implemented in devices,
- used as applications (user side),
- applied in networks,
- applied in data storage, cloud and back-end servers.

`PETs` may provide these basic privacy features:

- (P1) *anonymity*: user is not identifiable as the source of data (user is indistinguishable).
- (P2) *pseudonymity*: user is identifiable only to system parties (issuers), trades off between anonymity and accountability.
- (P3) *unlinkability*: actions of the same user cannot be linked together, and all sessions are mutually unlinkable.
- (P4) *untracebility*: user's credentials and/or actions cannot be tracked by system parties (issuers).
- (P5) *revocation*: a dedicated system party is able to remove person or its credential from the system.
- (P6) *data privacy*: stored and/or released information do not expose undesired properties, e.g. identities, user's vital data etc.

Further, `PETs` combine privacy features with common security features such as:

- (S1) *data confidentiality*: sensitive data are protected against eavesdropping and exposing by encryption techniques.
- (S2) *data authenticity and integrity*: data are protected against their lost or modification by the unauthorized entities.
- (S3) *authentication*: proof that a connection is established with an authenticated entity or access to services is granted only to authenticated entity .
- (S4) *non-repudiation*: proof that a data is signed by a certain entity (entity cannot deny this action).
- (S5) *accountability*: a user should have specific responsibilities.

Table 2. Categorization of Privacy Threats, Leakages, Attacks with Prevention Approaches and Affected IoT Areas

Privacy issue (threat/ leakage/ attack)	**Description**	**Prevention approaches**	**IoT areas**
Data over-collection threat	Unaware and/or superabundant collection of personal data	*Data minimization, data anonymization*	All IoT areas with data collection
Linkage threat	Disclosing unexpected results by different systems can lead to linkage of personal data by data correlation	*Data minimization, data anonymization, user awareness/informed consent transparency*	All IoT areas with data collection and dissemination
Identification threat	Associating a user identity with personal data, e.g., name, address, gender, physical signatures (voice, face)	*Data anonymization, identity management, data security*	All IoT areas with data collection and dissemination
Lifecycle transitions leakage	Leaking personal data from devices and systems in their lifecycle that are not under their control or by changing the ownership of smart things	*Data control, identity management, data security*	Smart cities, smart homes, IoV
Privacy-violating interactions and presentation leakage	Conveying and presenting private information through a public medium (voice, video screens) that leads to disclosure of user private information to an unwanted audience	*Data anonymization, user awareness/informed consent transparency*	Health care, smart cities
Localization leakage	Undesirable determining of a persons location by Global Positioning System (GPS) coordinates, IP addresses, latency, or cell phone location	*Data anonymization, data control*	Health care, IoV, smart cities
Behavioral leakage	Undesirable determining and recording a persons behavior through space and time.	*Data anonymization, data control*	IoV, smart cities, smart homes, smart grid
Tracking attack	Attackers can determine and record a persons movement through time and space (based on localization or behavioral leakages and user identification), e.g., data exploitation by criminals for robberies/kidnapping	*Data anonymization, data minimization, data control*	IoV, smart cities, smart homes
Profiling attack	Attackers can compile and analyze information about users in order to infer their personal interests by correlation with their profiles and data, e.g. exposing a targets life pattern, unsolicited personalized e-commerce, blackmailing	*Data minimization, data anonymization*	Health care, smart cities, IoV, smart grid
Inventory attack	Attackers can send various query requests to the object and analyze the related responses in order to collect special interests of users, e.g., unauthorized detection of health issues, burglaries, industrial espionage	*Data control, identity management, data security*	Health care, IoV, smart industry, IoT device exchanging
Eavesdropping Attack	Attackers can observe and eavesdrop communication in order to directly get private information and/or notification about a user's presence, i.e. detection some encrypted communications	*Data security, secure communication*	All IoT areas with data collection and dissemination
Identity-theft Attack	Attackers can steal user identity (credentials) and misuse his/her services, and/or harm his/her reputation	*Data security, identity management*	IoV, smart cities, healthcare, smart industry

As above, privacy (P1 - P6) and security (S1 - S5) features are only basic and common. Table 3 presents PETs categorized into 6 processes (data authenticity, user authentication, communication, computation/data processing, data storing and data dissemination), and provides a brief description of PETs, their privacy and security features and standards and/or examples of references for existed IoT implementations or the PET's consideration in IoT. Mentioned technologies may conduct and represent many various schemes that have different properties. Furthermore, this analysis for simplicity does not involve advanced and special features, e.g. malleability, no framing, transparency, and intervenability, which can be found in the special variants of PET schemes.

In addition, it is assumed that well-established techniques already provide principally native features such as soundness, correctness, unforgeability, completeness etc. Suitable and matured PETs for IoT applications are integrated into our proposed framework in the following Section 6.

6 Privacy-Preserving Framework for Internet of Things

In this section, we propose a general privacy-preserving framework for an IoT communication model. Our proposed novel framework is mainly based on general security and privacy requirements of IoT applications and potential privacy issues in IoT based services. The general concept of the proposed framework is depicted in Figure 3. The framework contains 4 initial processes, 6 privacy-preserving data procedures, and 4 general post-processes. The privacy preserving data procedures are mainly focused on embedding the PETs in IoT services (e.g. access control in smart cities/smart buildings, IoV data exchanging etc.). These framework processes can be applied linearly in time. Furthermore, we recommend suitable types of PETs in order to solve concrete privacy-issues in each detected area and aspect in the general IoT model.

Before employing concrete PETs into an IoT application, initial Privacy-by-Design strategies and procedures must be set and performed in order to be in line with privacy standards and principles, i.e., ISO/IEC 29100:2011, [57], [18]. The *initial processes* of the framework are defined as follows:

- **System Definition**: Define data flaws and data procedures for the concrete IoT application/system.
- **Privacy Analysis**: Analyze the privacy breaches and issues in the concrete IoT application/system.
- **Data Definition**: Define concrete datasets, user's vital and sensitive data that should be protected and set limitation.
- **Legal Definition**: Set and ensure purpose legitimacy, consents and information strategies in according to regulations and laws.

Then, the *technical processes* should be set and ensured by employing PETs in these 6 privacy-preserving data procedures:

1. **Privacy-preserving Information Collection**: The collection of data including some user-specific parameters (user location, user consumption, etc.)

Table 3. Categorization of Technical-based Privacy-enhancing Technologies and IoT-related References

Process	Technology name	Description	Privacy and security features	Standards and/or the examples of IoT-related references
Data authenticity	Blind Signatures (BS)	BS enable signers to disguise the content of a signed message.	P3-P4, P6, S2, S4	[ISO/IEC 18370], [34, 58]
	Group Signatures (GS)	GS offers privacy-preserving properties for signers who sign the messages on behalf of the group.	P2-P5, S2-S4	[ISO/IEC 20008], [15, 31, 12, 10]
	Ring Signatures (RS)	RS offers similar privacy-preserving properties as GS. It is computationally infeasible to determine which group members' keys were used to produce the signature.	P2-P5, S2-S4	[9, 54, 11]
User authentication	Attribute-Based Credentials (ABC)	ABC enable entities (users) to anonymously or pseudo-anonymously prove the possession of various personal attributes in order to get access to services. The solutions are often based on anonymous credentials and zero-knowledge protocols.	P2 - P6, S2 - S5	ISO/IEC 27551 [1, 37, 4, 46]
	Anonymous and Pseudonymous Authentication (A&PA)	A&PA enable entities (users) to anonymously or pseudo-anonymously authenticate in ICT systems. The authentication protocols have specific privacy features.	P1 - P4, S3	[ISO/IEC 20009], [ISO/IEC 29191], [7]
Communication	Onion Routing (OR)	Anonymous networks like Tor rely on passing through multiple nodes with a layer of encryption added at each node.	P1, P3, P4, S1, S2	[17, 3]
	Encrypted Communication (EC)	EC enables basic privacy protection of transmitted data against external observers. Methods are usually based on basic encryption, DTLS, VPNs, PGP, email encryption and so on.	P6, S1 - S4	[39], [30]
	Mix-networks (MixNets)	MixNets transport data via multiple relays with certain delays and cover traffic to mask statistical leaks that could trace messages.	P2	[51]
	Proxies and Crowds (P&C)	P&C approaches use intermediaries (proxy servers) in order to hide data senders. With Crowds a user is join a crowd and uses services anonymously.	P1, P2	[43]
Computation	Homomorphic Encryption (HE)	HE allows the performing of selected operations on encrypted data.	P6, S1, S2	[47, 28]
	Polymorphic Encryption and Pseudonymisation (PE&P)	PE&P provides the security and privacy infrastructure for big data analytics.	P2, P6, S1	[56]
	Multiparty Computations (MC)	MC enables several parties to jointly compute a function over their inputs, while at the same time keeping these inputs private.	P6, S5	[52, 32]
	Searchable Encryption (SE)	SE allows the performing of predefined searches on encrypted data located on untrusted third party without the need to decrypt.	P6, S1, S2	[26]
	Attribute-Based Encryption (ABE)	ABE is public-key encryption techniques in which users secret key and the ciphertext are dependent upon attributes. The attributes can be represented by geographic location, users age and account level (premium, standard, basic) in case of streaming services. Only a user with specific attributes can decrypt the ciphertext.	P6, S1, S2, S5	[38, 19]
Data Storing	Statistical Disclosure Control (SDC)	SDC techniques include tabular data protection, queryable database protection, microdata protection, etc. The goal is storing data (i.e., data set, data base or tabular) that preserve their statistical validity while protecting the privacy of each data subject.	P6, S5	[62, 24]
	Data Splitting (DS)	DS means partitioning a data set into fragments in such a way that the fragment considered in isolation is no longer sensitive. Each fragment is then stored in a different site.	P6	[20]
Data Dissemination	Differential Privacy (DP)	DP releases information that contains nothing about an individual while contains useful information about a population.	P6	[40]
	Syntactic Anonymization Techniques (SAT)	SAT merges general techniques to remove, suppress or generalize identifying information from data (images, text, voice, video, etc.), the de-identification methods (such as k-anonymity) under low-privacy requirements and location privacy methods by obfuscation and cloaking.	P1, P2, P6	[40] , [53]

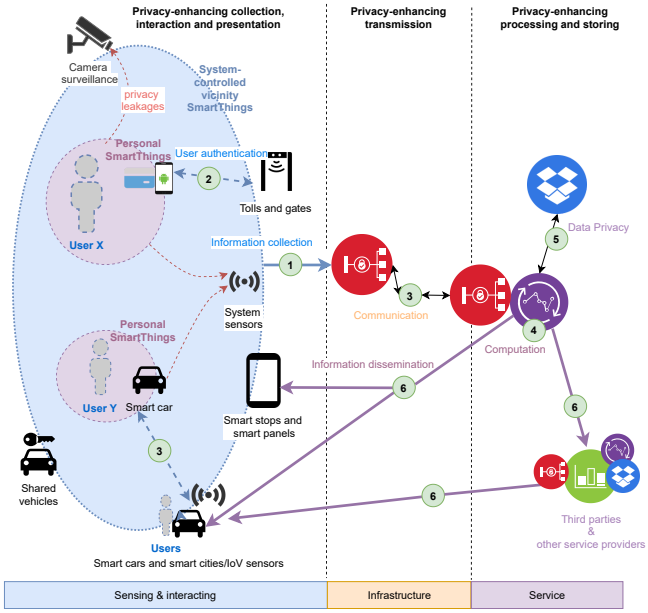

Fig. 3. The proposed privacy-preserving framework for IoT environment.

should ensure user privacy and data authenticity. Employing anonymous/pseudonymous digital signatures such as digital group signatures (`GS`) should provide data authenticity, non-repudiation and also hide users as sources of data in the group of members. This approach provides k-anonymity where k is the number of all members. The implementation of short (few KBs) group signatures (e.g. [10, 12, 31]) that need several asymmetric cryptographic operations could be feasible in IoT using small devices (i.e. mobiles, microcontrollers).

2. **Privacy-preserving User Authentication**: The privacy of users who access IoT services should be protected by privacy-preserving user authentication. `ABC` seems as very promising approach due to the support of various security and privacy features. Moreover, some efficient `ABC` schemes (e.g. [14, 46, 5]) are also suitable for constrained devices (e.g. existed smartcard implementation) that is point to the readiness of `ABC` for IoT. In case of smart safety systems, the user identification should be also based on PETs/ABC schemes and the verification of safety equipment can be done anonymously.
3. **Privacy-preserving Communication**: Collected and sensed data from vicinity and personal smart things should be securely transferred via a network infrastructure to a service area. Therefore, the communication should be protected by standard encryption techniques suitable for IoT and heterogeneous networks (e.g. `DTLS`, `wolfSSL`). In case of uploading or exchanging sensitive and anonymous user data, the communication relations should be protected by privacy-preserving communication techniques based on onion

routing, MixNets or broadcasting in order to provide source privacy, i.e. hide source IP address. Recently, the paper [3] has utilized the Tor Network for IoT. Moreover, anonymous digital signatures and GS can be used to ensure data authenticity and integrity without leaking the identity of a sender.

4. **Privacy-preserving Computation**: The back-end servers of IoT services or cloud infrastructures should perform privacy-preserving data processing. For privacy-preserving computation, there are many possible techniques and privacy-preserving options, such as HE, SW, ABE, MC, and PE&P. Using techniques such as homomorphic encryption is possible to perform some data analysis and keep data private for owners. Nonetheless, HE and SE methods could be less applicable to performance-constrained client nodes (see results in [47]). Therefore, these heavy computation operations should be performed at powerful back-end servers or clouds. On the other hand, fine-grained access control on encrypted outsourced data can be realized by ABE schemes. The work [19] shows the results of ABE on small devices with promising efficiency in terms of processing time and energy consumption.
5. **Privacy-preserving Data Storing**: A service area should store only necessary data in a privacy-preserving way. There are several SDC techniques (microdata protection, etc.) that enable users to store data and protect their privacy. These approaches lead to data minimization. Also, the data should be secured by standard methods (e.g. storage encryption). The implementation of SDC techniques should not be problematic on most IoT platforms and storages but data minimization should be done in a reasonable way without losing the important data for an analysis.
6. **Privacy-preserving Data Dissemination**: The results of data processing that are disseminated and presented back to users or to third parties should not contain any vital and/or private information about concrete users. The combination of presentation rules and data minimization strategies should be employed in order to keep user privacy.

After embedding PETs into data procedures, *post-processes* for sustainability and general management must be followed:

- **Evaluation**: The final application/service should be evaluated whether PETs and technical processes mitigate privacy and security issues.
- **Control**: The functionality of concrete privacy-preserving data procedures should be constantly controlled.
- **Monitoring**: The data visibility and transparency in the system should be ensured.
- **Compliance**: The compliance with the current regulations and laws should be checked, and the system should be able to demonstrate this.

7 Conclusion

This paper focuses on privacy protection in Intelligent Infrastructures and IoT applications. In this work, we detected privacy-requiring IoT applications, and

analyzed and categorized various privacy issues and privacy-enhancing technologies from the perspective of IoT. Based on the analyzed privacy breaches in IoT and privacy-enhancing technologies divided into 6 categories, a general framework was proposed that consists of 8 general processes and 6 technical privacy-preserving procedures. The presented framework should serve as a guideline for establishing privacy-preserving IoT applications and systems in line with privacy-by-design concepts. The particular applications that will benefit from the framework the most are identification systems, access control systems, smart safety systems, smart-grids and health care.

Acknowledgment

This paper is supported by the Ministry of Industry and Trade grant # FV20354, the TACR project TL02000398 and European Union's Horizon 2020 research and innovation programme under grant agreement No 830892, project SPARTA. For the research, infrastructure of the SIX Center supported by National Sustainability Program under grant LO1401 was used.

References

1. Alpár, G., Batina, L., Batten, L., Moonsamy, V., Krasnova, A., Guellier, A., Natgunanathan, I.: New directions in iot privacy using attribute-based authentication: Position paper (2016)
2. Atamli, A.W., Martin, A.: Threat-based security analysis for the internet of things. In: International Workshop on Secure Internet of Things. pp. 35–43. IEEE (2014)
3. Baumann, F.W., Odefey, U., Hudert, S., Falkenthal, M., Breitenbücher, U.: Utilising the tor network for iot addressing and connectivity. In: Proceedings of the 8th International Conference on Cloud Computing and Services Science (CLOSER 2018). pp. 27–34. SciTePress (Mar 2018)
4. Bernal Bernabe, J., Hernandez-Ramos, J.L., Skarmeta Gomez, A.F.: Holistic privacy-preserving identity management system for the internet of things. Mobile Information Systems 2017 (2017)
5. Camenisch, J., Drijvers, M., Dzurenda, P., Hajny, J.: Fast keyed-verification anonymous credentials on standard smart cards. In: Dhillon, G., Karlsson, F., Hedström, K., Zúquete, A. (eds.) ICT Systems Security and Privacy Protection. pp. 286–298. Springer International Publishing, Cham (2019)
6. Cha, S.C., Hsu, T.Y., Xiang, Y., Yeh, K.H.: Privacy enhancing technologies in the internet of things: Perspectives and challenges. IEEE Internet of Things Journal (2018)
7. Chatzigiannakis, I., Vitaletti, A., Pyrgelis, A.: A privacy-preserving smart parking system using an iot elliptic curve based security platform. Computer Communications 89, 165–177 (2016)
8. Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J.H., Metayer, D.L., Tirtea, R., Schiffner, S.: Privacy and data protection by design-from policy to engineering. arXiv preprint arXiv:1501.03726 (2015)
9. Debnath, A., Singaravelu, P., Verma, S.: Privacy in wireless sensor networks using ring signature. Journal of King Saud University-Computer and Information Sciences 26(2), 228–236 (2014)

10. Derler, D., Slamanig, D.: Highly-efficient fully-anonymous dynamic group signatures. In: Proceedings of the 2018 on Asia Conference on Computer and Communications Security. pp. 551–565. ACM (2018)
11. Dwivedi, A.D., Srivastava, G., Dhar, S., Singh, R.: A decentralized privacy-preserving healthcare blockchain for iot. Sensors 19(2), 326 (2019)
12. Emura, K., Hayashi, T.: A light-weight group signature scheme with time-token dependent linking. In: Lightweight Cryptography for Security and Privacy. pp. 37–57. Springer (2015)
13. Finn, R.L., Wright, D., Friedewald, M.: Seven types of privacy. In: European data protection: coming of age, pp. 3–32. Springer (2013)
14. Hajny, J., Dzurenda, P., Malina, L.: Attribute-based credentials with cryptographic collusion prevention. Security and Communication Networks 8(18), 3836–3846 (2015)
15. He, D., Chen, C., Bu, J., Chan, S., Zhang, Y., Guizani, M.: Secure service provision in smart grid communications. IEEE Communications Magazine 50(8), 53–61 (2012)
16. Henze, M., Hermerschmidt, L., Kerpen, D., Häußling, R., Rumpe, B., Wehrle, K.: User-driven privacy enforcement for cloud-based services in the internet of things. In: 2014 International Conference on Future Internet of Things and Cloud. pp. 191–196. IEEE (2014)
17. Hoang, N.P., Pishva, D.: A tor-based anonymous communication approach to secure smart home appliances. In: 2015 17th International Conference on Advanced Communication Technology (ICACT). pp. 517–525. IEEE (2015)
18. Hoepman, J.H.: Privacy design strategies. In: IFIP International Information Security Conference. pp. 446–459. Springer (2014)
19. Jahan, M., Seneviratne, S., Chu, B., Seneviratne, A., Jha, S.: Privacy preserving data access scheme for iot devices. In: 2017 IEEE 16th International Symposium on Network Computing and Applications (NCA). pp. 1–10. IEEE (2017)
20. Kelarev, A.V., Yi, X., Cui, H., Rylands, L.J., Jelinek, H.F.: A survey of state-of-the-art methods for securing medical databases. AIMS Medical Science 5(1), 1–22 (2018)
21. Kong, Q., Lu, R., Ma, M., Bao, H.: A privacy-preserving sensory data sharing scheme in internet of vehicles. Future Generation Computer Systems 92, 644–655 (2019)
22. Li, C., Palanisamy, B.: Privacy in internet of things: From principles to technologies. IEEE Internet of Things Journal 6(1), 488–505 (Feb 2019)
23. Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., Zhao, W.: A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. IEEE Internet of Things Journal 4(5), 1125–1142 (2017)
24. Liu, F., Li, T.: A clustering-anonymity privacy-preserving method for wearable iot devices. Security and Communication Networks 2018 (2018)
25. Lopez, J., Rios, R., Bao, F., Wang, G.: Evolving privacy: From sensors to the internet of things. Future Generation Computer Systems 75, 46–57 (2017)
26. Ma, M., He, D., Kumar, N., Choo, K.K.R., Chen, J.: Certificateless searchable public key encryption scheme for industrial internet of things. IEEE Transactions on Industrial Informatics 14(2), 759–767 (2017)
27. Ma, Y., Wu, Y., Li, J., Ge, J.: Apcn: A scalable architecture for balancing accountability and privacy in large-scale content-based networks. Information Sciences (2019)

28. Mai, V., Khalil, I.: Design and implementation of a secure cloud-based billing model for smart meters as an internet of things using homomorphic cryptography. Future Generation Computer Systems 72, 327–338 (2017)
29. Malina, L., Hajny, J., Fujdiak, R., Hosek, J.: On perspective of security and privacy-preserving solutions in the internet of things. Computer Networks 102, 83–95 (2016)
30. Malina, L., Srivastava, G., Dzurenda, P., Hajny, J., Fujdiak, R.: A secure publish/subscribe protocol for internet of things. In: Proceedings of the ARES 2019. ACM (2019)
31. Malina, L., Vives-Guasch, A., Castellà-Roca, J., Viejo, A., Hajny, J.: Efficient group signatures for privacy-preserving vehicular networks. Telecommunication Systems 58(4), 293–311 (2015)
32. von Maltitz, M., Carle, G.: Leveraging secure multiparty computation in the internet of things. arXiv preprint arXiv:1806.02144 (2018)
33. Medaglia, C.M., Serbanati, A.: An overview of privacy and security issues in the internet of things. In: The internet of things, pp. 389–395. Springer (2010)
34. Nieto, A., Rios, R., Lopez, J.: Digital witness and privacy in iot: Anonymous witnessing approach. In: 2017 IEEE Trustcom/BigDataSE/ICESS. pp. 642–649. IEEE (2017)
35. Patton, M., Gross, E., Chinn, R., Forbis, S., Walker, L., Chen, H.: Uninvited connections: a study of vulnerable devices on the internet of things (iot). In: IEEE Joint Intelligence and Security Informatics Conference. pp. 232–235. IEEE (2014)
36. Porambage, P., Ylianttila, M., Schmitt, C., Kumar, P., Gurtov, A., Vasilakos, A.V.: The quest for privacy in the internet of things. IEEE Cloud Computing 3(2), 36–45 (2016)
37. Put, A., De Decker, B.: Attribute-based privacy-friendly access control with context. In: International Conference on E-Business and Telecommunications. pp. 291–315. Springer (2016)
38. Ramos, J.L.H., Bernabé, J.B., Skarmeta, A.F.: Towards privacy-preserving data sharing in smart environments. In: Eighth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing. pp. 334–339. IEEE (2014)
39. Raza, S., Trabalza, D., Voigt, T.: 6lowpan compressed dtls for coap. In: 2012 IEEE 8th International Conference on Distributed Computing in Sensor Systems. pp. 287–289. IEEE (2012)
40. Rodríguez, C.R.G., et al.: Using differential privacy for the internet of things. In: IFIP International Summer School on Privacy and Identity Management. pp. 201–211. Springer (2016)
41. Rodriguez, J.D.P., Schreckling, D., Posegga, J.: Addressing data-centric security requirements for iot-based systems. In: 2016 International Workshop on Secure Internet of Things (SIoT). pp. 1–10. IEEE (2016)
42. Roman, R., Zhou, J., Lopez, J.: On the features and challenges of security and privacy in distributed internet of things. Computer Networks 57(10), 2266–2279 (2013)
43. Rothenpieler, P., Altakrouri, B., Kleine, O., Ruge, L.: Distributed crowd-sensing infrastructure for personalized dynamic iot spaces. In: Proceedings of the First International Conference on IoT in Urban Space. pp. 90–92. ICST (Institute for Computer Sciences, Social-Informatics and (2014)
44. Seliem, M., Elgazzar, K., Khalil, K.: Towards privacy preserving iot environments: A survey. Wireless Communications and Mobile Computing 2018 (2018)
45. Sen, A.A.A., Eassa, F.A., Jambi, K., Yamin, M.: Preserving privacy in internet of things: a survey. International Journal of Information Technology 10(2), 189–200 (2018)

46. Sene, I., Ciss, A.A., Niang, O.: I2pa: An efficient abc for iot. Cryptography 3(2), 16 (2019)
47. Shafagh, H., Hithnawi, A., Droescher, A., Duquennoy, S., Hu, W.: Talos: Encrypted query processing for the internet of things. In: Proceedings of the 13th ACM conference on embedded networked sensor systems. pp. 197–210. ACM (2015)
48. Sicari, S., Rizzardi, A., Grieco, L.A., Coen-Porisini, A.: Security, privacy and trust in internet of things: The road ahead. Computer networks 76, 146–164 (2015)
49. Solanas, A., Patsakis, C., Conti, M., Vlachos, I.S., Ramos, V., Falcone, F., Postolache, O., Pérez-Martínez, P.A., Di Pietro, R., Perrea, D.N., et al.: Smart health: a context-aware health paradigm within smart cities. IEEE Communications Magazine 52(8), 74–81 (2014)
50. Srinivasan, V., Stankovic, J., Whitehouse, K.: Protecting your daily in-home activity information from a wireless snooping attack. In: Proceedings of the 10th international conference on Ubiquitous computing. pp. 202–211. ACM (2008)
51. Staudemeyer, R.C., Pöhls, H.C., Wójcik, M.: The road to privacy in iot: beyond encryption and signatures, towards unobservable communication. In: 2018 IEEE 19th International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM). pp. 14–20. IEEE (2018)
52. Tso, R., Alelaiwi, A., Rahman, S.M.M., Wu, M.E., Hossain, M.S.: Privacy-preserving data communication through secure multi-party computation in healthcare sensor cloud. Journal of Signal Processing Systems 89(1), 51–59 (2017)
53. Ullah, I., Shah, M.A., Wahid, A., Mehmood, A., Song, H.: Esot: a new privacy model for preserving location privacy in internet of things. Telecommunication Systems 67(4), 553–575 (2018)
54. Vance, N., Zhang, D.Y., Zhang, Y., Wang, D.: Privacy-aware edge computing in social sensing applications using ring signatures. In: IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS). pp. 755–762. IEEE (2018)
55. Vasilomanolakis, E., Daubert, J., Luthra, M., Gazis, V., Wiesmaier, A., Kikiras, P.: On the security and privacy of internet of things architectures and systems. In: Proceedings of SIoT. pp. 49–57. IEEE (2015)
56. Verheul, E.R., Jacobs, B., Meijer, C., Hildebrandt, M., de Ruiter, J.: Polymorphic encryption and pseudonymisation for personalised healthcare. IACR Cryptology ePrint Archive 2016, 411 (2016)
57. Voigt, P., Von dem Bussche, A.: The eu general data protection regulation (gdpr). A Practical Guide, 1st Ed., Cham: Springer International Publishing (2017)
58. Wang, X., Jiang, J., Zhao, S., Bai, L.: A fair blind signature scheme to revoke malicious vehicles in vanets. Computers, Materials & Continua 58(1), 249–262 (2019)
59. Xu, W., Zhou, H., Cheng, N., Lyu, F., Shi, W., Chen, J., Shen, X.: Internet of vehicles in big data era. IEEE/CAA Journal of Automatica Sinica 5(1), 19–35 (2017)
60. Yang, Y., Wu, L., Yin, G., Li, L., Zhao, H.: A survey on security and privacy issues in internet-of-things. IEEE Internet of Things Journal 4(5), 1250–1258 (2017)
61. Yao, Z., Ge, J., Wu, Y., Jian, L.: A privacy preserved and credible network protocol. Journal of Parallel and Distributed Computing (2019)
62. Yavari, A., Panah, A.S., Georgakopoulos, D., Jayaraman, P.P., van Schyndel, R.: Scalable role-based data disclosure control for the internet of things. In: 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS). pp. 2226–2233. IEEE (2017)

63. Zhou, R., Zhang, X., Wang, X., Yang, G., Wang, H., Wu, Y.: Privacy-preserving data search with fine-grained dynamic search right management in fog-assisted internet of things. Information Sciences 491, 251–264 (2019)
64. Ziegeldorf, J.H., Morchon, O.G., Wehrle, K.: Privacy in the internet of things: threats and challenges. Security and Communication Networks 7(12), 2728–2742 (2014)