# Towards Privacy and Secure IoT Services Based on Privacy-Enhancing Technologies

Lukas Malina*, Gautam Srivastava†, Petr Dzurenda*, Jan Hajny*, and Sara Ricci*
* Department of Telecommunications, Brno University of Technology, Brno, Czech Republic
† Department of Mathematics and Computer Science, Brandon University, Brandon, Canada
e-mail: {malina, dzurenda, hajny, ricci}@feec.vutbr.cz, and srivastavag@brandonu.ca

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

***Index Terms*—Authentication; Cryptography; Evaluation; Identification; Internet of Things; Privacy; Privacy-Enhancing Technologies; Security.**

## I. 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. The general overview of IoT environments and applicable scenarios are depicted in Figure 1.

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. It is essential during the design and application stages 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 [1], 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 [2] 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 [2] 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**;

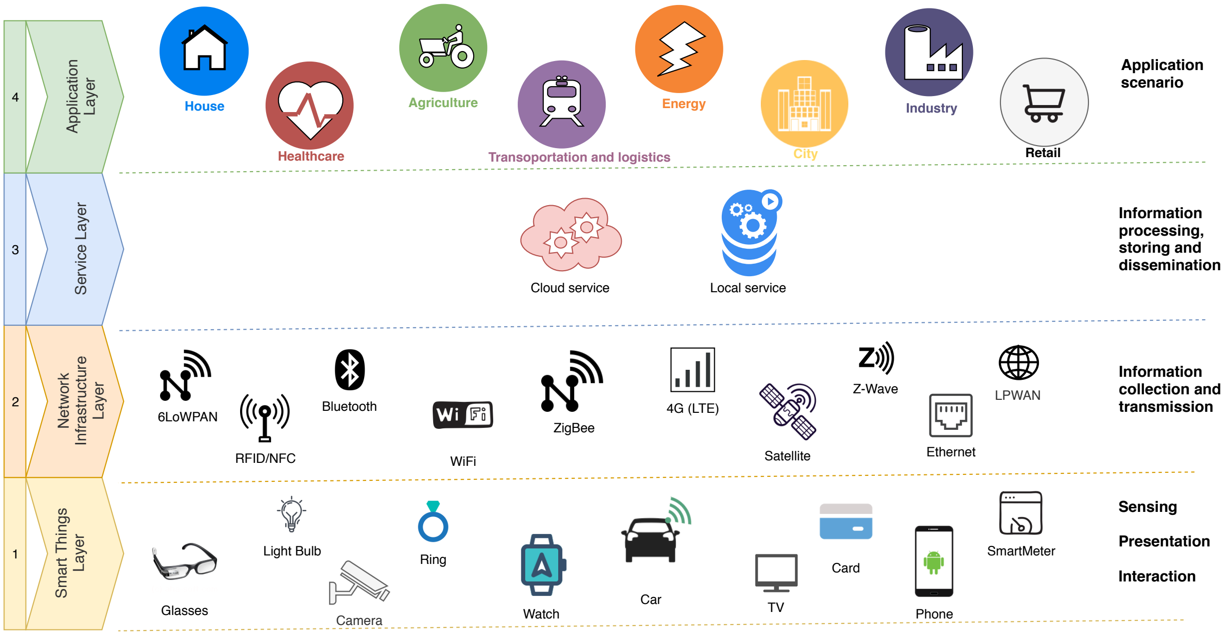


Fig. 1. The IoT enviroment and application areas.

- **Transparency-enhancing techniques**;
- **Intervenability-enhancing techniques**.

In this paper, we focus on privacy-preserving techniques that can be employed in IoT environments.

### A. 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 [3]. 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 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.

### B. 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 [4]. 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.

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 Section IV.

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.

The rest of the paper is organized as follows. In Section II we describe the state of the art. We follow this in Section III by exploring specific use cases of IoT where users have or may experience privacy issues. Section IV presents privacy issues in IoT. Next, in Section V we deal with the categorization and

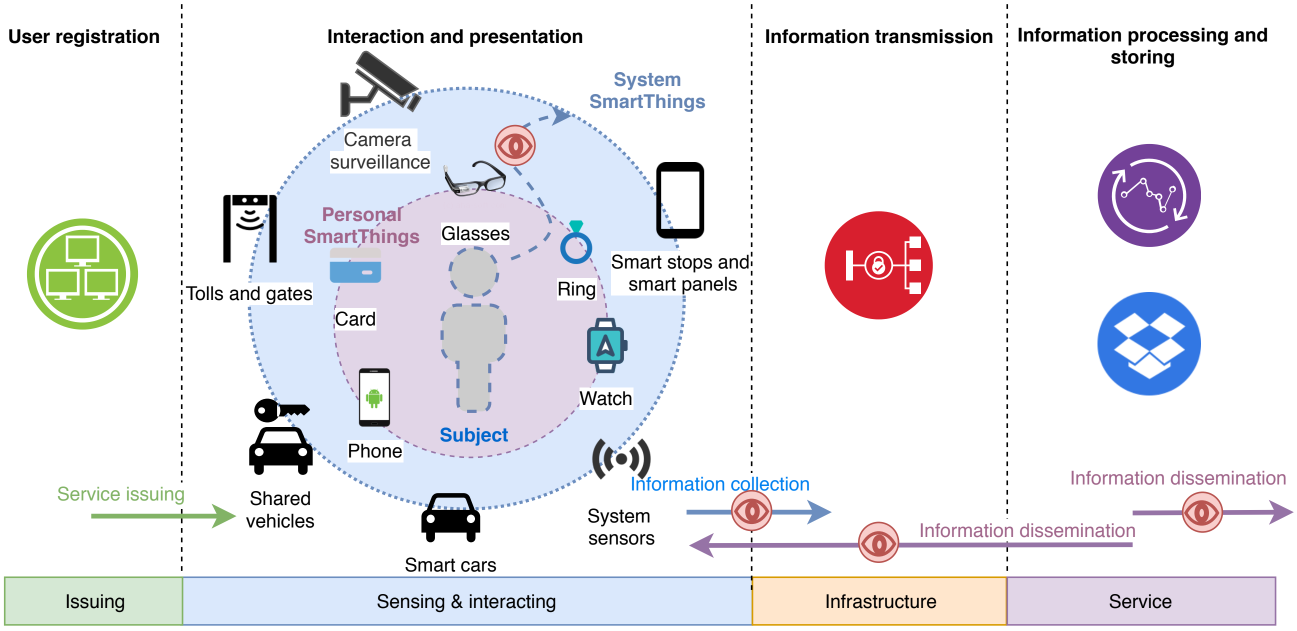


Fig. 2. The IoT communication model and privacy breaches.

assessment of PETs in IoT. Section VI presents our proposal of general privacy-preserving framework for IoT. Lastly, we give some concluding remarks in Section VII.

## II. State of the Art

There are plenty of interesting studies and survey papers focusing on security and privacy in IoT [5], [6], [7], [8]. Furthermore, there are surveys and study papers that focus solely on privacy in IoT. Some examples are given in[9], [10], [11], [12], [13], [14].

Seliem *et al.* review existing research and propose solutions to rising privacy concerns from a multiple viewpoint to identify the risks and mitigations in [11]. 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 [13]. 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` [15]. 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` [14]. 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 [12], 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 III.

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.

## III. 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 user's 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 devices systems that were exposed online, and that $12,000$ of them belonged to one healthcare organization [16]. 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. [17]. 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 a observations from a last-mile Internet service provider or other adversary located on the Wide Area Network (`WAN`). The `FATS` attack demonstrates that traffic analyses attacks in the style of `FATS` are as effective for the current generation of consumer IoT devices as they were for sensor networks a decade ago.

To really hit home with another 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 really 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 [18]. 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 her medical information and the other with her 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).

Important social challenges stem from the necessity to adapt Smart City services to the specific characteristics of every user [19]. 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 [20], [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 [22], 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.

We summarize our findings listing areas of IoT, some concrete applications, and the privacy concerns in Table I. The privacy concerns used match the list from [23], 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 I
IoT AREAS WITH THE EXAMPLE OF APPLICATIONS AND PRIVACY CONCERNS [23]

| 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 |

## IV. Categorization of Privacy Issues: Threats, Leakages and Attacks in IoT Environment

In this section, we categorize privacy issues and present brief descriptions, potential prevention approaches and menaced IoT areas. Security attacks and privacy threats in IoT have been analyzed in various studies [24], [4], [25], [12]. Lopez *et al.* detect 3 IoT privacy problems: user privacy, content privacy and context privacy [10]. Furthermore, there have been seven privacy threat categories in IoT given in [4], [12]. 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 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 II, 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.

## V. 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 backend 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.

TABLE II
CATEGORIZATION OF PRIVACY THREATS, LEAKAGES AND ATTACKS

| 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 the 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 lifecycles that are not under their control or by changing the ownership of the smart thing | *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 disclose user private information to an unwanted audience | *Data anonymization, user awareness/informed consent transparency* | Health care, smart cities |
| Localization leakage | Undesirable determining a persons location by, e.g., 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 persons movement through time and space (based on localization or behavioral leakages and user identification), e.g., data exploitation by criminals for burglaries, kidnaps | *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 the 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 the special interests of an user from the item, 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 presence, i.e. detection some encrypted communications | *Data security, secure communication* | All IoT areas with data collection and dissemination |
| Identity-theft Attack | Attackers can theft user identity (credentials) and misuse his/her services, or/and harm his/her reputation | *Data security, identity management* | IoV, smart cities, healthcare, smart industry |

- (P6) *data privacy*: stored 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 has specific responsibilities.

Above privacy (P1 - P6) and security (S1 - S5) features are only basic and common. Table III presents PETs categorized into 5 areas, and provide the briefly description of PETs, their privacy and security features and standards and/or examples of references for existed IoT implementations or 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 VI.

TABLE III
Categorization of Technical-based Privacy-enhancing Technologies for IoT

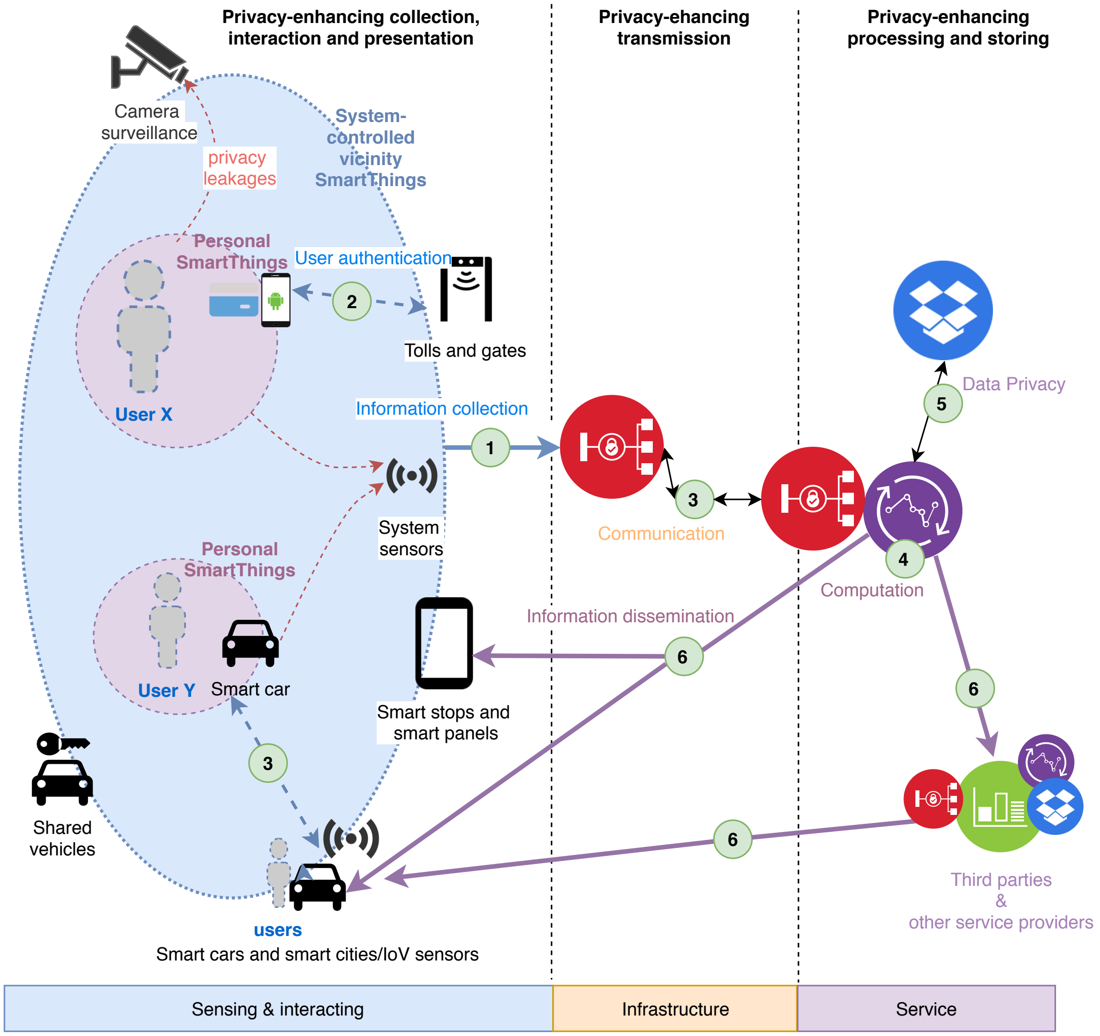
| Process/area | Technology Name | Description | Privacy and security features | Standards and/or the examples of IoT-related references |
|---|---|---|---|---|
| Data authenticity | Blind Signatures (BS) | BS enable signers to blind the content of a signed message. | P3-P4, P6, S2, S4 | [ISO/IEC 18370] , [26] |
| | Group Signatures (GS) | GS offer privacy-preserving properties for signers who sign the messages on behalf of the group. | P2-P5, S2-S4 | [ISO/IEC 20008], [27], [28] |
| | Ring Signatures (RS) | RS offer similar privacy-preserving properties as GS. It is computationally infeasible to determine which of the group members' keys was used to produce the signature. | P2-P5, S2-S4 | [29] |
| User authentication | Attribute-Based Credentials (ABC) | ABC enable entities (users) to anonymously or pseudonymously 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 [30], [31] [32] |
| | Anonymous and Pseudonymous Authentication (A&PA) | A&PA enable entities (users) to anonymously or pseudonymously authenticate in ICT systems. The authentication protocols have specific privacy features. | P1 - P4, S3 | [ISO/IEC 20009], [ISO/IEC 29191], [33] |
| 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 | [34] |
| | Encrypted Communication (EC) | EC enable 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 | [35], [36] |
| | Mix-networks (MixNets) | MixNets transport data via multiple relays with certain delays and cover traffic to mask statistical leaks that could trace messages. | P2 | [37] |
| | 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 | [38] |
| Computation/Processing | Homomorphic Encryption (HE) | HE allows to perform selected operations on encrypted data. | P6, S1, S2 | [39] |
| | Polymorphic Encryption and Pseudonymisation (PE&P) | PE&P provide the security and privacy infrastructure for big data analytics. | P2, P6, S1 | [11] |
| | Multiparty Computations (MC) | MC enable several parties to jointly compute a function over their inputs, while at the same time keeping these inputs private. | P6, S5 | [40] |
| | 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 | [41] |
| | Searchable Encryption (SE) | SE allows performing predefined searches on encrypted data located on untrusted third party without the need to decrypt. | P6, S1, S2 | [39] |
| | Attribute-Based Encryption (ABE) | ABE is public-key encryption technique 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 | [42] |
| Data privacy/Storing | Statistical Disclosure Control (SDC) | SDC techniques include tabular data protection, queryable database protection, microdata protection, differential privacy etc. The goal is releasing data (i.e., data set, data base or tabular) that preserve their statistical validity while protecting the privacy of each data subject. | P6, S5 | [43] |
| | Privacy-preserving Data Mining (PDM) | PDM are methods that allow extracting information from data while preserving privacy of the subject of whom the data are referred to. | P6 | [44], [41] |
| | General Privacy-enhancing Data Techniques (GPDT) | GPDT merge general techniques to remove 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 | [45] , [46] |

## VI. 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. 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, [3], [1]. 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,



Privacy-enhancing collection, interaction and presentation
Privacy-enhancing transmission
Privacy-enhancing processing and storing
Camera surveillance
privacy leakages
System-controlled vicinity SmartThings
Personal SmartThings
User authentication
2
Tolls and gates
User X
Information collection
1
System sensors
3
Communication
Data Privacy
5
4
Computation
Personal SmartThings
User Y
Smart car
Information dissemination
6
Smart stops and smart panels
6
3
Shared vehicles
6
Third parties & other service providers
users
Smart cars and smart cities/IoV sensors
Sensing & interacting
Infrastructure
Service

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

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.) 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.
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 are also suitable constrained devices (e.g. existed smartcard implementation) that is point to the readiness of ABC for IoT.
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. In this scenario, anonymous digital signatures and GS can be used to ensure data authenticity and integrity.
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.

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, differential privacy, etc.) that enable users to store data and protect their privacy. These approaches that lead to data minimization and obfuscation should be used. Also, the data should be secured by standard methods (e.g. storage encryption).

6) **Privacy-preserving Information Dissemination**: The results of data processing that are disseminated and presented back to users or to third parties should not contain any vital or private information about concrete users. The combination of presentation rules and data minimization strategies should be employed.

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.

## VII. 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, a general framework was proposed that consists of 8 general processes and 6 technical privacy-preserving procedures. The presented framework should serve as a guidance for establishing privacy-preserving IoT applications and systems in line with privacy-by-design concepts.

## Acknowledgment

This paper is supported in part by European Union's Horizon 2020 research and innovation program under grant agreement No 830892, project SPARTA. The National Sustainability Program under Grant no. LO1401 and the Technology Agency of the Czech Republic under Legal and technical tools for privacy protection in cyberspace project (TL02000398) financed the research described in this article. For the research, the infrastructure of the SIX Center was used.

## References

[1] J.-H. Hoepman, "Privacy design strategies," in *IFIP International Information Security Conference*. Springer, 2014, pp. 446–459.

[2] G. Danezis, J. Domingo-Ferrer, M. Hansen, J.-H. Hoepman, D. L. Metayer, R. Tirtea, and S. Schiffner, "Privacy and data protection by design-from policy to engineering," *arXiv preprint arXiv:1501.03726*, 2015.

[3] P. Voigt and A. Von dem Bussche, "The eu general data protection regulation (gdpr)," *A Practical Guide, 1st Ed., Cham: Springer International Publishing*, 2017.

[4] 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.

[5] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Computer Networks*, vol. 57, no. 10, pp. 2266–2279, 2013.

[6] 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.

[7] L. Malina, J. Hajny, R. Fujdiak, and J. Hosek, "On perspective of security and privacy-preserving solutions in the internet of things," *Computer Networks*, vol. 102, pp. 83–95, 2016.

[8] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142, 2017.

[9] P. Porambage, M. Ylianttila, C. Schmitt, P. Kumar, A. Gurtov, and A. V. Vasilakos, "The quest for privacy in the internet of things," *IEEE Cloud Computing*, vol. 3, no. 2, pp. 36–45, 2016.

[10] J. Lopez, R. Rios, F. Bao, and G. Wang, "Evolving privacy: From sensors to the internet of things," *Future Generation Computer Systems*, vol. 75, pp. 46–57, 2017.

[11] M. Seliem, K. Elgazzar, and K. Khalil, "Towards privacy preserving iot environments: A survey," *Wireless Communications and Mobile Computing*, vol. 2018, 2018.

[12] S.-C. Cha, T.-Y. Hsu, Y. Xiang, and K.-H. Yeh, "Privacy enhancing technologies in the internet of things: Perspectives and challenges," *IEEE Internet of Things Journal*, 2018.

[13] A. A. A. Sen, F. A. Eassa, K. Jambi, and M. Yamin, "Preserving privacy in internet of things: a survey," *International Journal of Information Technology*, vol. 10, no. 2, pp. 189–200, 2018.

[14] C. Li and B. Palanisamy, "Privacy in internet of things: From principles to technologies," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 488–505, Feb 2019.

[15] E. Vasilomanolakis, J. Daubert, M. Luthra, V. Gazis, A. Wiesmaier, and P. Kikiras, "On the security and privacy of internet of things architectures and systems," in *2015 International Workshop on Secure Internet of Things (SIoT)*. IEEE, 2015, pp. 49–57.

[16] M. Patton, E. Gross, R. Chinn, S. Forbis, L. Walker, and H. Chen, "Uninvited connections: a study of vulnerable devices on the internet of things (iot)," in *2014 IEEE Joint Intelligence and Security Informatics Conference*. IEEE, 2014, pp. 232–235.

[17] V. Srinivasan, J. Stankovic, and K. Whitehouse, "Protecting your daily in-home activity information from a wireless snooping attack," in *Proceedings of the 10th international conference on Ubiquitous computing*. ACM, 2008, pp. 202–211.

[18] M. Henze, L. Hermerschmidt, D. Kerpen, R. Häußling, B. Rumpe, and K. Wehrle, "User-driven privacy enforcement for cloud-based services in the internet of things," in *2014 International Conference on Future Internet of Things and Cloud*. IEEE, 2014, pp. 191–196.

[19] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in internet-of-things," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1250–1258, 2017.

[20] W. Xu, H. Zhou, N. Cheng, F. Lyu, W. Shi, J. Chen, and X. Shen, "Internet of vehicles in big data era," *IEEE/CAA Journal of Automatica Sinica*, vol. 5, no. 1, pp. 19–35, 2017.

[21] Q. Kong, R. Lu, M. Ma, and H. Bao, "A privacy-preserving sensory data sharing scheme in internet of vehicles," *Future Generation Computer Systems*, vol. 92, pp. 644–655, 2019.

[22] A. Solanas, C. Patsakis, M. Conti, I. S. Vlachos, V. Ramos, F. Falcone, O. Postolache, P. A. Pérez-Martínez, R. Di Pietro, D. N. Perrea *et al.*, "Smart health: a context-aware health paradigm within smart cities," *IEEE Communications Magazine*, vol. 52, no. 8, pp. 74–81, 2014.

[23] R. L. Finn, D. Wright, and M. Friedewald, "Seven types of privacy," in *European data protection: coming of age*. Springer, 2013, pp. 3–32.

[24] C. M. Medaglia and A. Serbanati, "An overview of privacy and security issues in the internet of things," in *The internet of things*. Springer, 2010, pp. 389–395.

[25] A. W. Atamli and A. Martin, "Threat-based security analysis for the internet of things," in *2014 International Workshop on Secure Internet of Things*. IEEE, 2014, pp. 35–43.

[26] A. Nieto, R. Rios, and J. Lopez, "Digital witness and privacy in iot: Anonymous witnessing approach," in *2017 IEEE Trustcom/BigDataSE/ICESS*. IEEE, 2017, pp. 642–649.

[27] D. He, C. Chen, J. Bu, S. Chan, Y. Zhang, and M. Guizani, "Secure service provision in smart grid communications," *IEEE Communications Magazine*, vol. 50, no. 8, pp. 53–61, 2012.

[28] L. Malina, A. Vives-Guasch, J. Castellà-Roca, A. Viejo, and J. Hajny, "Efficient group signatures for privacy-preserving vehicular networks," *Telecommunication Systems*, vol. 58, no. 4, pp. 293–311, 2015.

[29] A. Debnath, P. Singaravelu, and S. Verma, "Privacy in wireless sensor networks using ring signature," *Journal of King Saud University-Computer and Information Sciences*, vol. 26, no. 2, pp. 228–236, 2014.

[30] G. Alpár, L. Batina, L. Batten, V. Moonsamy, A. Krasnova, A. Guellier, and I. Natgunanathan, "New directions in iot privacy using attribute-based authentication: Position paper," 2016.

[31] A. Put and B. De Decker, "Attribute-based privacy-friendly access control with context," in *International Conference on E-Business and Telecommunications*. Springer, 2016, pp. 291–315.

[32] J. Bernal Bernabe, J. L. Hernandez-Ramos, and A. F. Skarmeta Gomez, "Holistic privacy-preserving identity management system for the internet of things," *Mobile Information Systems*, vol. 2017, 2017.

[33] I. Chatzigiannakis, A. Vitaletti, and A. Pyrgelis, "A privacy-preserving smart parking system using an iot elliptic curve based security platform," *Computer Communications*, vol. 89, pp. 165–177, 2016.

[34] N. P. Hoang and D. Pishva, "A tor-based anonymous communication approach to secure smart home appliances," in *2015 17th International Conference on Advanced Communication Technology (ICACT)*. IEEE, 2015, pp. 517–525.

[35] S. Raza, D. Trabalza, and T. Voigt, "6lowpan compressed dtls for coap," in *2012 IEEE 8th International Conference on Distributed Computing in Sensor Systems*. IEEE, 2012, pp. 287–289.

[36] L. Malina, G. Srivastava, P. Dzurenda, J. Hajny, and R. Fujdiak, "A secure publish/subscribe protocol for internet of things," in *Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES 2019)*. ACM, 2019.

[37] R. C. Staudemeyer, H. C. Pöhls, and M. Wójcik, "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)*. IEEE, 2018, pp. 14–20.

[38] P. Rothenpieler, B. Altakrouri, O. Kleine, and L. Ruge, "Distributed crowd-sensing infrastructure for personalized dynamic iot spaces," in *Proceedings of the First International Conference on IoT in Urban Space*. ICST (Institute for Computer Sciences, Social-Informatics and , 2014, pp. 90–92.

[39] J. D. P. Rodriguez, D. Schreckling, and J. Posegga, "Addressing data-centric security requirements for iot-based systems," in *2016 International Workshop on Secure Internet of Things (SIoT)*. IEEE, 2016, pp. 1–10.

[40] R. Tso, A. Alelaiwi, S. M. M. Rahman, M.-E. Wu, and M. S. Hossain, "Privacy-preserving data communication through secure multi-party computation in healthcare sensor cloud," *Journal of Signal Processing Systems*, vol. 89, no. 1, pp. 51–59, 2017.

[41] A. V. Kelarev, X. Yi, H. Cui, L. J. Rylands, and H. F. Jelinek, "A survey of state-of-the-art methods for securing medical databases," *AIMS Medical Science*, vol. 5, no. 1, pp. 1–22, 2018.

[42] J. L. H. Ramos, J. B. Bernabé, and A. F. Skarmeta, "Towards privacy-preserving data sharing in smart environments," in *2014 Eighth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*. IEEE, 2014, pp. 334–339.

[43] F. Liu and T. Li, "A clustering-anonymity privacy-preserving method for wearable iot devices," *Security and Communication Networks*, vol. 2018, 2018.

[44] K. Kenthapadi, I. Mironov, and A. G. Thakurta, "Privacy-preserving data mining in industry," in *Proceedings of the Twelfth ACM International Conference on Web Search and Data Mining*. ACM, 2019, pp. 840–841.

[45] C. R. G. Rodríguez *et al.*, "Using differential privacy for the internet of things," in *IFIP International Summer School on Privacy and Identity Management*. Springer, 2016, pp. 201–211.

[46] I. Ullah, M. A. Shah, A. Wahid, A. Mehmood, and H. Song, "Esot: a new privacy model for preserving location privacy in internet of things," *Telecommunication Systems*, vol. 67, no. 4, pp. 553–575, 2018.