**D2.1. State of the Art Analysis for Personal Data Security in IoT**

**PARFAIT - Personal dAta pRotection FrAmework for IoT**

**Editors**: Gemalto

**Contributors**:

**Reviewer**:

|  |  |  |  |
| --- | --- | --- | --- |
| **WP2** | | Scenarios, Specifications, and Requirements Definitions | |
| **Leader** | | Gemalto | |
| **Task** | | T2.1 State of the Art Analysis | |
| **Deliverable number** | | D2.1. State of the Art Analysis for Personal Data Security in IoT | |
| **Type** | | Doc | |
| **Author** | | BEIA, SIS, University of La Rochelle, Gemalto | |
| **Other contributors** | |  | |
| **Keywords** | | State-Of-The-Art, Guidances | |
| **Date of delivery** | | 2018-10-06 | |
| **Draft history** (to be removed on publication) | | | | |
| V.0.1 |  | | Initial Version | |
| V.0.6 | Oct. 2018 | |  | |
| V.0.7 | Nov. 2018 | | ULR | |
| V.1.0 | 21/11/2018 | | Final V1.0 version | |

Table of Contents

[1 Introduction 5](#_Toc528828911)

[1.1 Overview 5](#_Toc528828912)

[1.2 PARFAIT Components 6](#_Toc528828913)

[2 IoT Devices and IoT-based Environments 8](#_Toc528828914)

[2.1 IoT devices 8](#_Toc528828915)

[2.1.1 IoT device management 9](#_Toc528828916)

[2.2 IoT-based environments 10](#_Toc528828917)

[2.2.1 IoT device connectivity and networking 10](#_Toc528828918)

[2.2.2 IoT device security 10](#_Toc528828919)

[2.2.3 IoT-based environments 10](#_Toc528828920)

[2.3 IoT Device Trends and Anticipated Growth 14](#_Toc528828921)

[3 Security in IoT-based environments from both software and hardware standpoints 15](#_Toc528828922)

[3.1 Effect of IoT features on security and privacy 15](#_Toc528828923)

[3.1.1 The Security Features of IoT 16](#_Toc528828924)

[3.1.2 Challenges with Security Principles 16](#_Toc528828925)

[3.2 Security issues in IoT 16](#_Toc528828926)

[3.2.1 Software Standpoint 17](#_Toc528828927)

[3.2.2 Hardware Standpoint 17](#_Toc528828928)

[3.2.3 Embedded Secure Element (eSE) 20](#_Toc528828929)

[3.3 Security Threats 21](#_Toc528828930)

[4 User data management in IoT-based environment 23](#_Toc528828931)

[4.1 Cloud Information Architectures 23](#_Toc528828932)

[4.1.1 Infrastructure as a Service (IaaS) 23](#_Toc528828933)

[4.1.2 Platform as a service 24](#_Toc528828934)

[4.1.3 Software as a Service 24](#_Toc528828935)

[4.1.4 Data Dispersion 24](#_Toc528828936)

[4.2 Information Management 24](#_Toc528828937)

[4.2.1 The Data Security Lifecycle 25](#_Toc528828938)

[4.2.2 Information Governance 26](#_Toc528828939)

[4.3 Data Security 26](#_Toc528828940)

[4.3.1 Internal Data Migration 27](#_Toc528828941)

[4.3.2 Movement to Cloud 27](#_Toc528828942)

[4.3.3 Secure Data Transfer within/to the Cloud 27](#_Toc528828943)

[5 User Data Protection and Privacy Preservation 29](#_Toc528828944)

[5.1 Privacy and User Data Protection Approaches 29](#_Toc528828945)

[5.1.1 User privacy concerns 29](#_Toc528828946)

[5.1.2 User Data Protection and Privacy preservation methods in IoT applications 30](#_Toc528828947)

[5.1.3 Data anonymization methods 31](#_Toc528828948)

[5.1.4 Data Minimization and Data Shelf Life 31](#_Toc528828949)

[5.1.5 Big Data and privacy 32](#_Toc528828950)

[5.2 User Data Protection Tools 32](#_Toc528828951)

[5.2.1 Personal Information Management System 32](#_Toc528828952)

[5.3 User Data Protection Regulations 34](#_Toc528828953)

[5.3.1 US versus Europe regulation for user privacy protection 34](#_Toc528828954)

[5.3.2 The European Regulation: General Data Protection Regulation (GDPR) 35](#_Toc528828955)

[6 User Data Protection and Privacy Preservation: Best Practices 40](#_Toc528828956)

[6.1 Process 40](#_Toc528828957)

[6.2 User Data Exploitation 41](#_Toc528828958)

[6.3 User Data Back-up 42](#_Toc528828959)

[6.4 Privacy by design 43](#_Toc528828960)

[6.4.1 The 7 Foundational Principles of PbD 43](#_Toc528828961)

[6.4.2 Privacy by design and GDPR 43](#_Toc528828962)

[7 Conclusion 44](#_Toc528828963)

**List of Figures**

[Figure ‎1‑1 IoT architecture 5](#_Toc528828964)

[Figure ‎1‑2 PARFAIT project value chain 7](#_Toc528828965)

[Figure ‎2‑1. AWS IoT platform 11](#_Toc528828966)

[Figure ‎2‑2 A security framework for embedded IoT and IIoT devices that provides protection against a wide variety of cyberattacks [52] 13](#_Toc528828967)

[Figure ‎2‑3 An implementation of the required elements to provide security in embedded devices [52] 13](#_Toc528828968)

[Figure ‎2‑4 IoT device trends and anticipated growth 14](#_Toc528828969)

[Figure ‎2‑5 High-profile architecture 15](#_Toc528828970)

[Figure ‎3‑1 Architecture regarding medical IoT 19](#_Toc528828971)

[Figure ‎4‑1 Cloud computing data life cycle 25](#_Toc528828972)

**List of Tables**

[Table ‎2‑1 Awair specifications. 9](#_Toc528828973)

[Table ‎4‑1 Consumer DRM vs. Enterprise DRM 29](#_Toc528828974)

[Table ‎7‑1 Comparison between US-EU privacy principles 35](#_Toc528828975)

# Introduction

## Overview

The Internet of Things (IoT) concept refers to the usage of standard Internet protocols to allow for human-to-thing interaction and thing-to-thing communication. IoT emerged from IT frameworks and this led to addressing the cybersecurity only from their point of view. Many times, these approaches are not adequate to provide a solution for the particular security and flexibility requirements of the industrial processes’ operations. Specific aspects need to be considered for industrial IoT (IIoT) networks, such as what technologies can be implemented and where, and which threats it should address. Several industry groups have already proposed multi-layered approaches, frameworks and sets of controls for securing devices and assets in IIoT networks, and some technology for protecting connected devices and networks already exists [44].

The Internet of Things (IoT) [1] represents a model surfaced from the widespread advances in information and communication technology (ICT). The comprehensive IoT framework includes a system of objects or devices like sensors to be handled, embedded processors and radio frequency identification (RFID) labels, supplied to the IoT gateway and the server. When describing an IoT system, three layers are defined: the perception layer, the network layer, and the applications layer. Figure ‎1‑1 presents how these layers are combined within an IoT architecture.

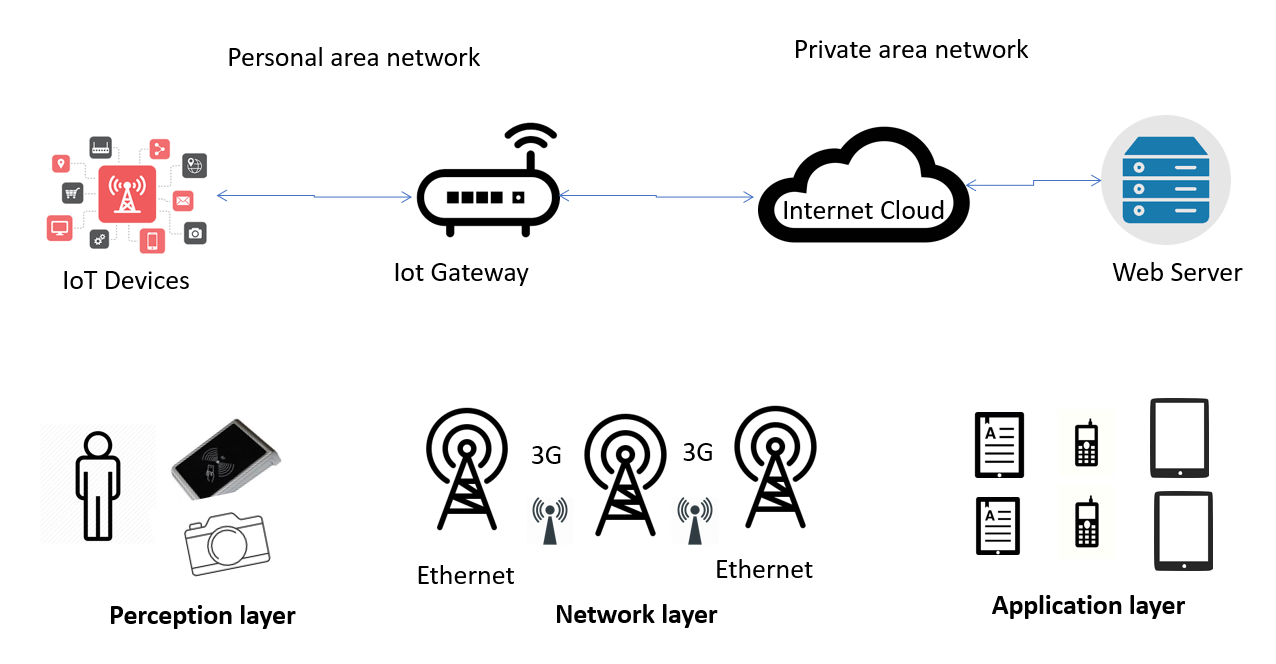


Figure ‎1‑1 IoT architecture

IoT is used to develop the purposes of the Internet’s initial version by augmenting the objects’ capabilities to interconnect. An IoT framework facilitates the information sharing between the users and the connected objects from the physical environment. Using communication technologies such as wireless fidelity (Wi-Fi), RFID, near field communication (NFC), Bluetooth, internet protocol (IP), actuators, sensors, electronic product code (EPC), and wireless sensor networks (WSNs), IoT can transmit the desired data. The major goal IoT wants to achieve is to facilitate the unique identification and access of users to control the “things” from wherever and whenever they desire through the Internet.

Besides, from the data point of view, IoT technologies raise also privacy concerns, particularly when it comes to IoT-based applications intended to natural individuals or people, such as home automations, location-based services, drive tracking, etc.

In this context, the right to personal privacy is one of the fundamental human rights. Security and privacy functions allow developing trustworthy application environments in which people can trust the apps they are using, and the apps are forbidden to abuse the users by placing them under surveillance and to take non-legitimate benefits from their personal data.

Security and privacy concerns in IoT applications have not been considered thoroughly in application design and development methods. In near future, we may face an aggravation in the situation given the following observations[[1]](#footnote-1):

* The increasing number of connected objects already invaded home and/or professional spaces (around 26 billion devices by 2020),
* Impact of security concerns on customers’ purchase decision for IoT products,
* 47% of organizations do not ensure any kind of data privacy information regarding the data generated from their IoT products,
* Only 48% of companies focus on securing their IoT products from the beginning of the product development phase,
* A significant number of software vulnerabilities can be addressed if organizations adhere to secure coding standards and best practices.

“Privacy by design” provides general principles to ensure user privacy protection. The state of the art encompasses all the efforts and work carried out so far in the domain. It includes regulations (national, European, and international), standards, guidelines, implementation approaches, methods, architectures, limitations and drawbacks, challenges in the field, etc.

## PARFAIT Components

PARFAIT project’s main goal is to develop a platform for protecting personal data in Internet of Things applications. Another goal of the project is to decrease the complexity of integrating and deploying services in today’s Internet of Things technology by providing interoperable software libraries, tools and SDK elements.

It is a strong ambition of the project to define interoperability and security/privacy methodologies, rules and guidelines to make recommendations for the policy makers. Defined methodologies and policies will be used as the keystones to develop libraries, tools and SDKs which will construct the foundation layer for domain specific Internet of Things service frameworks and connected application ecosystems.

Internet of Things is a new paradigm, which aims at changing the human – machine interaction by providing a new communication medium based on distributed computing and connectivity. Along with the potential benefits, Internet of Things also has strong challenges. The most important challenges Internet of Things is facing today are the interoperability and security/privacy issues. These challenges put crucial limitations and prevent the full advancement and growth in the market.

The PARFAIT project aims at finding solutions to these challenges and opening the way to connected Internet of Things application ecosystems. Two emerging domains will be addressed by the project, namely, Personal Information Management, and Smart Home Services.

The following Figure ‎1‑2 summarises the boundaries of PARFAIT project in terms of stakeholders and components to be developed.

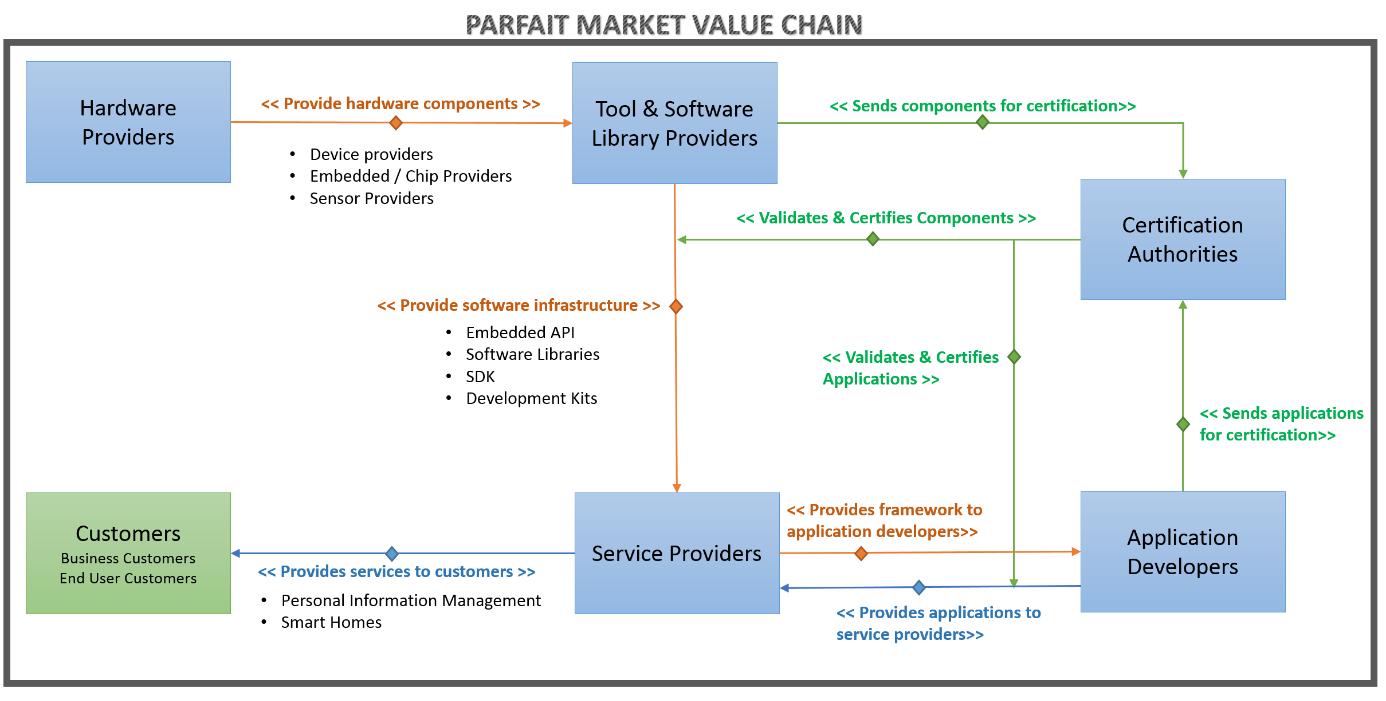


Figure ‎1‑2 PARFAIT project value chain

The state of the art covers the main topics in regards with the following components:

* **Guidelines, Specifications and Standardization** aims at defining a software development methodology, a domain model, a corresponding architecture and a set of guidelines for developing secure, privacy preserving and interoperable IoT applications.
* **Privacy and Security Framework** defines and implements the software libraries, Software Development Kits and tools based on the methodology and guidelines defined in the guidelines, specifications and standardization layer.
* **Thematic Service Frameworks** develop domain specific service framework led by the industrial service provider consortium partners.
* **Application Space** defines the connected ecosystems built around the thematic frameworks using applications developed by consortium partners.

This state of the art encompasses the following topics:

* IoT devices and IoT-based environments,
* Security in IoT-based environments,
* User data management in IoT-based environments,
* User data protection and privacy protection,
* Best Practices for user data protection and privacy protection.

# IoT Devices and IoT-based Environments

## IoT devices

The devices of IoT are “nonstandard” computing instruments that usually connect through wireless to a network and have the role and ability to gather and transmit data. These devices go beyond the usual ones, like desktops, laptops, smartphones and tablets, and can be controlled remotely.

IoT devices function in an environment in order to automate home and industry tasks and to communicate available sensor data to its users, businesses or others. Considering the target public, these devices can be categorized in three groups: consumer, enterprise and industrial.

The consumer category includes smart TVs, smart appliances, smart wearables and toys. On the other hand, smart meters, security systems or smart city technologies belong to enterprise and industrial IoT. For example, appliances for monitoring traffic and weather conditions, smart air conditioning, smart thermostats, smart lighting and smart security contribute to the enterprise and industrial IoT area.

One simple example of a smart home is that a user arriving home can make the car communicate with the garage to open the door. Inside, the thermostat is set to the desired temperature, the lighting is set to a lower intensity with a specific color for relaxation because it was transmitted that the user had a busy and stressful day.

In an enterprise work area, the smart sensors located in a conference room can help with booking an appropriate room in size, availability and features. When the meeting attendees will enter in that room they will be welcomed by the set preferences, for example, the temperature, lights, open PowerPoint etc.

Another example regarding IoT devices for smart home is the smart door lock. There are many possibilities, including remotely controlling the access of the door with the help of a phone. The door can be opened by enabling proximity sensors, for example Bluetooth and NFC, whenever an authorized user approaches the door. When creating a smart lock there are some elements that have to be considered. First, it should be determined by the connectivity type (Wi-Fi, Bluetooth, NFC or Cellular). Also, the compatibility with other connected devices should be checked. On the market already exist similar solutions [2] , few of them being the following: “[Schlage Sense](https://www.amazon.com/Schlage-Sense-Deadbolt-Latitude-Interior/dp/B01JJU8P9E)” from Apple Homekit, “[August Smart Lock Pro](https://www.amazon.com/August-Smart-Lock-Pro-Generation/dp/B0765JNS2D)” to use with Amazon Alexa, “[Kwikset 910](https://www.amazon.com/Kwikset-SmartCode-Electronic-SmartThings-featuring/dp/B004F1B24I/) ” for Samsung SmartThings, “August” from iTunes, “Kwikset Kevo” for Android App and many others.

As smart home devices there can be enumerated the following:

**Echo Spot** from Amazon [3] is a smart alarm clock that can be placed anywhere around the house. It uses far-field voice recognition, can be used to see music lyrics, weather forecasts, do shopping lists, listen to audiobooks and a lot more;

**August: Smart Lock** [4] has a place between the leaders of smart lock spaces. It can tell the user whether the door is locked and closed. It can be set to give access to anyone, for a few minutes, hours, weeks, depending on the user’s needs. It requires iOS (9.0 or higher) or Android (5.0 or higher);

**Nest Thermostat** [5] is designed to make the home smart and energy efficient. It lights up to show the temperature, weather or time and has far sight capabilities, so the user can see it across the room;

**Awair Glow** [6] represents a smart plug that can track air quality. It can track toxins and chemicals in the air. Its specifications are listed in the following table:

Table ‎2‑1 Awair specifications.

|  |  |
| --- | --- |
| Sensors | * Temperature ranging from -40 up to 125°; * Humidity ranging from 0 to 95% +/- 2%p; * CO2 ranging from 0 to 4000 ppm +/- 75 ppm; * Chemicals (VOCs): 0 to 2014 ppb. |
| System requirements | * Wi-Fi connection; * Smartphone or tablet with support for Bluetooth 4.0, iOS (8 or later) and Android (Jelly Bean 4.3 or later). |
| Wireless | * Wi-Fi connection: 802.11 b/g/n @2.4 GHz; * Bluetooth 4.0. |
| Power | * 100 ~125 AC, 50/60 Hz |

**CUJO** [7]is a smart firewall for home. It has the role of analyzing local network traffic data in real time and sends statistics on the data obtained and send it to the cloud for further analysis. At the end, ***CUJO*** will notify the user if there are anomalies taking place in the network.

**Keen Home** [8]is another interesting smart product for climate control and energy management. It has the role of modifying a rooms’ temperature by creating a room-zoomed system that balances the home’s temperature.

**Netatmo Welcome** [9] is a smart device for home security. The user can receive intruder alerts to their smartphone, receive custom alerts that distinguish between intruders and friends or family. It can also send alerts when the system detects alarms from Smoke Detector.

### IoT device management

IoT management addresses important topics like security, interoperability, processing capabilities, scalability and availability. The management helps with integrating, organizing, monitoring or remotely managing internet-enabled devices at different scales, with critical features to maintain the health, connectivity and security of the IoT devices.

Among these features can be mentioned:

* registration;
* authentication / authorization;
* configuration;
* provisioning;
* monitor and diagnose;
* troubleshooting.

Protocols for device management include Open Mobile Alliance’s Device Management (OMA DM) and Lightweight Machine-to-Machine (OMA LwM2M). Such device management services and software are available from vendors like Microsoft, Amazon, Bosch Software Innovations, Software AG etc.

## IoT-based environments

### IoT device connectivity and networking

There are many connectivity and communications options, depending on a large number of internet-enabled devices and on how that specific application is deployed. Most used communications protocols include CoAP, DTLS and MQTT. IPv6, LPWAN, Zigbee, Bluetooth Low Energy, Z-Wave, RFID and NFC belong to wireless protocols. Also, for device connectivity, what can be used are cellular, satellite, Wi-Fi and ethernet technologies.

For every particular IoT application, characteristics like power consumption, range, bandwidth have to be considered when choosing the protocol used. In order to share the data they collect, IoT devices can be connected to a gateway or some similar device which can store data, analyze it or sent it for a cloud analysis.

### IoT device security

In October 2016 a distributed denial-of-service attack affected DNS servers in the US, disrupting services worldwide. This issue was traced to hackers infiltrating networks through IoT devices, some wireless routers and connected cameras.

In this case, the source of the problem was the use of default passwords on the corrupt devices. As first measures, it is suggested to use strong passwords, authentication and identity management, network segmentation, encryption and cryptography.

Regarding these concerns, the FBI released a public announcement [FBI Alert Number I-091015-PSA](https://whatis.techtarget.com/definition/FBI-Alert-Number-I-091015-PSA) in September 2015 where they outline the risk of IoT devices as well as countermeasures and protection recommendations.

### IoT-based environments

IoT platforms [10] fill the gap between device sensors and data networks. These platforms connect the data networks to sensors and provide insight to users and developers. Not only big tech companies but also startups began to venture into IoT platform development.

**AWS IoT** has as main features a registry for recognizing devices, an SDK for devices, Device Shadows for persistent device state during intermittent connections, Secure Device Gateway to allow device communication through MQTT, HTTP or WebSockets and Rules Engine for inbound message evaluation. The AWS IoT Device SDK represents a set of client libraries to authenticate, connect and exchange messages. Using this platform, presented in figure Figure ‎2‑1, developers can connect multiple applications ranging from automobiles to turbines or smart home lights.

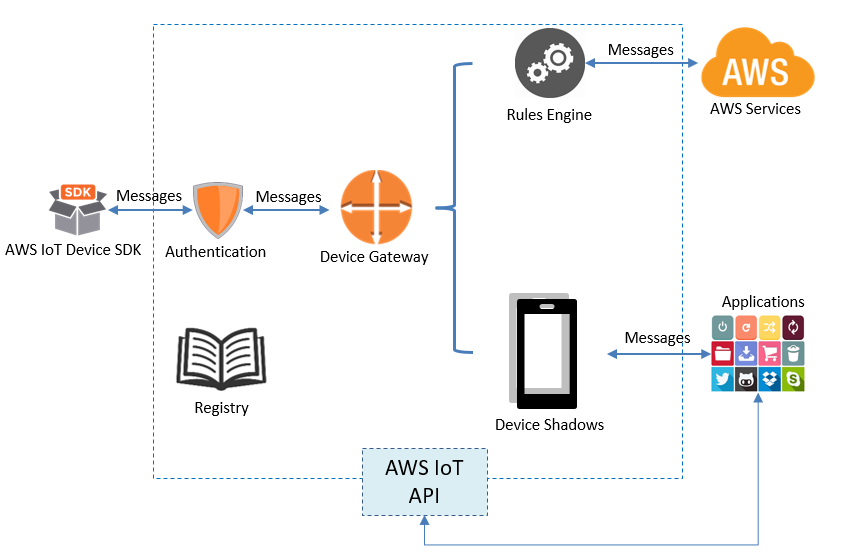


Figure ‎2‑1. AWS IoT platform

The features brought by **Microsoft** platform are device shadowing, a rules engine, identity registry and information monitoring. Azure Stream Analytics can process massive amounts of information generated by sensors in real-time.

Google Cloud Platform has also important characteristics in IoT, some of them being accelerating the business, speeding up devices, cutting costs with Cloud service, partner ecosystem.

Another platform on the market is ThingWorx IoT Platform. Its creators say that it enables creating and deploying games rapidly, solutions and experiences for the new smart connected world.

This platform is designed for enterprise application development and has popular features such as:

* easy connectivity for the devices of the platform;
* removing complexity in IoT development;
* possibility to share platform between developers for rapid growth;
* integrating machine learning for complex big data analytics;
* deployment on Cloud, embedded or on-premise solutions.

**IBM Watson** also has put on the market a big IoT platform. It is backed by IBM’s hybrid cloud platform as a service (PaaS) development platform and enables for developers an easy deployment of IoT applications. Some of its features are Device Management, Secure Communications, Real-Time Data Exchange, Weather Data Service, Data Storage and Data sensors.

The sixth platform presented is **Artik from Samsung Electronics**, which provides end-to-end platform for the smart products and services. Artik’s objective is to take care of the security, offering services such as Artik Module, Cloud, Security and ecosystem. Other important features are:

* The easy to use Cloud;
* Modules are built for performance and security;
* Security ensures protection from hacking.

**Cisco IoTCoud Connect** is a platform made for mobile operators with features like voice and data connectivity, SIM lifecycle management, IP session control, billing and reporting.

Later on, Cisco partnered with Farmer’s Federation in Australia to provide IoT agriculture solutions.

Another interesting platform is **HP Platform (Hewlett Packard)**. While it can be deployed in Cloud and also locally, HPE Universal of Things is a successful platform used in smart cities and in the automobile industry.

A few of its services are listed below:

* Secure Monetization;
* Data Analytics;
* Application Designer and Marketplace;
* Platform Architecture.

The IoT platform from Salesforce is focused on customer engagement and has features like:

* Sales;
* Services;
* Marketing;
* Apps.

Other platforms that made their way through the IoT world are [11]: Data by Bsquare, Mindsphere by Siemens, Ayla Network by Ayla, Bosh IoT Suite, IoT Carriots, Oracle Integrated Cloud, General Electric’s Predix, MBED IoT Device platform, Mosaic (LTI), Mocana, Kaa.

For **SCADA applications**, several telemetry solutions, like RealiteQ [48] or Skkynet [49], ensure remote data is transmitted using at least standard security procedures: no static IP, SSL, at least 128 hash-code S-key, no transparent connection, password encryption, blocking risky connections etc. RealiteQ comes with a complete set of solutions for industrial process interconnection consisting of iCex, a gateway acting as data aggregation and producer, COMP (Central Online Management Portal) for defining security and user permissions and enabling process interconnection, and UI, a browser-based user interface. The main disadvantages are the fact that the solution is proprietary and the lack of flexibility regarding the integration with other applications. Skkynet provides a similar secure data interconnection solution that uses open protocols used in process automation (OPC, Modbus, DDE etc.) over secure channels to connect remote sites or devices. The most common interconnection type is between PCs having their Cogent application, but industrial communication gateways that include an ETK driver were also developed to facilitate direct device connection.

At the plant level, IIoT is becoming more accessible through specific interfaces for industrial controllers. A good starting point to **identify IoT solutions for industrial applications** is IoT ONE, a portal presenting available suppliers, software and hardware solutions and case studies [50], grouped based on application keywords and making it easy to identify solutions fit to a specific application requirement. Many well know solution providers in this domain come with proprietary solutions: Siemens has the IOT2000 gateway, Allen Bradley has the IoT Connector, Phoenix Contact has the Cloud IoT gateway, Seneca has the LET’S platform, Wago has the IoT connectors etc. All these solutions focus on open connectivity and allow interoperability with their older product versions, but with basic solutions for ensuring communication security: encryption (usually TLS), access control and identity protection.

As mentioned in [51], researchers from IBM Security and data security firm Threatcare analyzed security aspects for sensor hubs from three companies—Libelium, Echelon, and Battelle. The researchers found a total of 17 vulnerabilities in products from these companies, including eight critical flaws. These include guessable default passwords that could make it easy for an attacker to access a device, along with bugs that could allow an attacker to inject malicious software commands and others that would allow an attacker to sidestep authentication checks. After this study was published all he companies provided patches to solve these vulnerabilities.

An important player in the IIoT security frameworks providers is Iconlabs [52]. They introduced the Internet of Secure Things concept and provided tools to support their recommendations. Their solution, the Floodgate Security Framework (FSF), provides a building block for creating secure embedded devices. Floodgate Security Framework modules are available as individual products or as an integrated framework for embedded Linux or any RTOS.

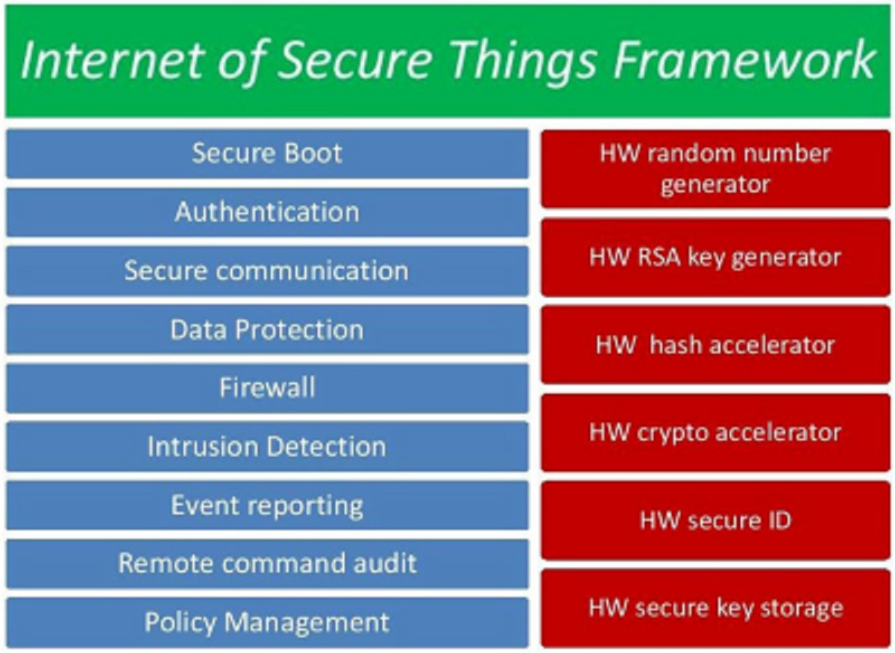


Figure ‎2‑2 A security framework for embedded IoT and IIoT devices that provides protection against a wide variety of cyberattacks [52]

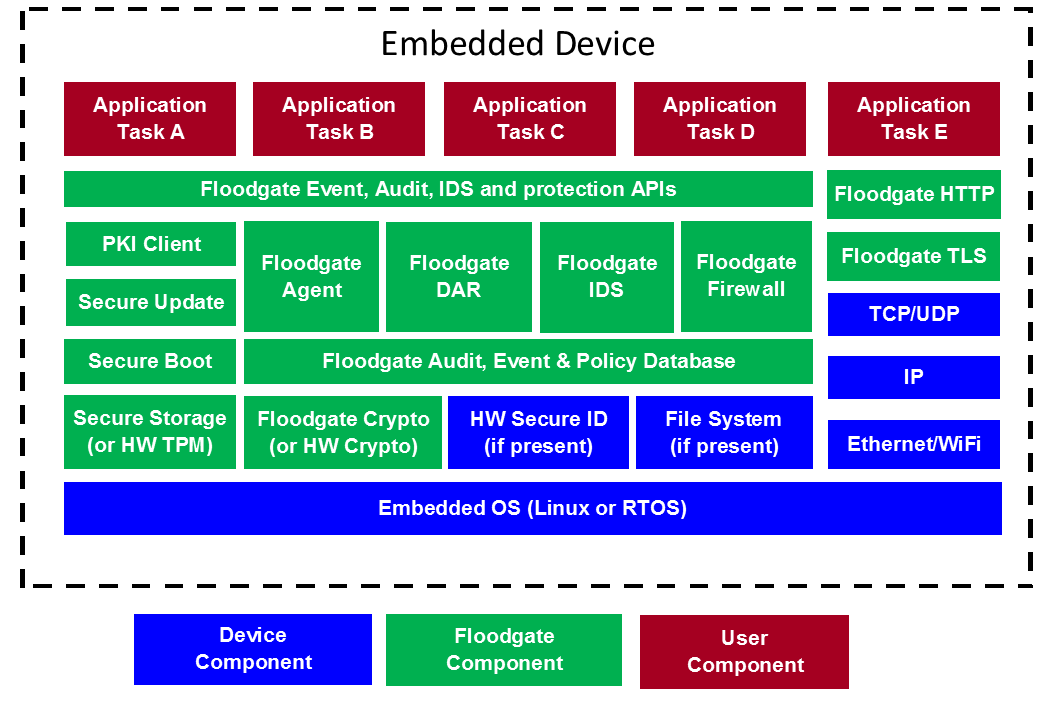


Figure ‎2‑3 An implementation of the required elements to provide security in embedded devices [52]

Kiaora is an open standard and open source IoT security solution initiated by Verisign for Eclipse developers [53]. It is based on IETF DNS-SD and IEFT DNS-SEC standard.

## IoT Device Trends and Anticipated Growth

An estimated number for IoT devices [12] is 8.4 billion in 2017, with a 31% increase compared to 2016. Intel numbered a grow from 2 billion in 2016 to 200 billion by year 2020, but if computers and tablets are not part of the equation then we remain with 20.8 billion connected devices by 2020, as seen from figure Figure ‎2‑4.

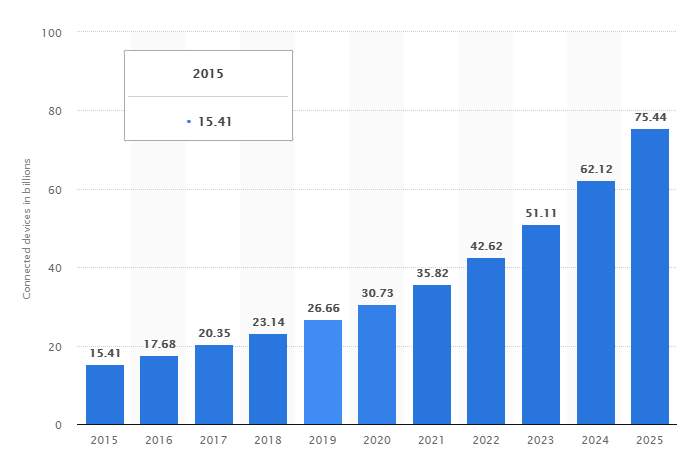


Figure ‎2‑4 IoT device trends and anticipated growth

Further, some innovative IoT devices are going to be listed and also their vulnerabilities.

The Belkin WeMo motion sensor and switch kit [13] connect to the Internet via Wi-Fi and allow the user to command the power socket for any electrical home instrument like room heater, coffee machine or desk lamp. This device was easily able to be attacked by ﬁrstly conducting a Simple Service Discovery Protocol (SSDP) to get the WeMo device’s IP address and the ports it is listening on. Afterwards, the Simple Object Access Protocol (SOAP) commands and their arguments supported by this device were acquired. Then, the attacker can allow remote-access on the device by signing up as an authentic user and by sending a relevant SOAP-formatted POST command. The attacker will then have remote access to the device from anywhere.

The Nest smoke-alarm issues reports and alerts to the user’s mobile application, giving them assurance that their house is secured regarding of their location. Still, it comes supplied with sensors that distinguish between motion and light, which can tell when the owner enters a room or if the lights are turned on/off. These abilities produce a privacy concern to those who feel that they are being followed within their home. But, the eavesdroppers cannot read the communications, because all information exchanges with the Nest smoke-alarm are encrypted.

To Withings Smart Baby Monitor an IP camera has been connected. It permits the owner to monitor their baby’s activity through an application installed on the phone. Wi-Fi packets exchanged between the baby monitor and the router have been analyzed. All the data is in plain-text, yet authorization to the camera still requires a server to send a prior access token. A “man-in-the-middle” (MITM) attack has been conducted. The victim’s app authenticates itself to the server and gets the session id and afterwards, the connection is hacked using ARP poisoning which allows the attacker to recover the source’s IP address into his hands, therefore to have access to the camera feed.

The Withings Smart Body Analyzer is a performant scale which can measure heart rate, body fat and Body Mass Index (BMI) besides weight. Through Wi-Fi or Bluetooth, it can connect to the Internet by pairing with an application, namely Withings Health Mate. Findings show that the owner’s personal data (gender, name, age, height, weight) is transmitted in plain-text over the communication channel. Also, by capturing Bluetooth packets, the scales sends a secret key and its MAC address, that are both utilized to provide an MD5 digest utilized by the server for authentication. The digest can be easily recreated by capturing the two details, facilitating an attacker to disguise its intrusive authentication to the device.

An entity entitled “Security Management Provider” (SMP) has been developed and described in the paper “Network-Level Security and Privacy Control for Smart-Home IoT Devices” [13]. It introduces the extra level of security into the equation, such as adding the suitable access control rules which safeguard a particular IoT device. Figure Figure ‎2‑5 presents the SMP interacting with the Internet Service Provider (ISP) through dynamic APIs on a side and with the home users on the other side through simple Graphical User Interfaces (GUIs). A content provider like Google, Facebook, Linkedin, etc. can also take this role to deliver improved and more secured services.

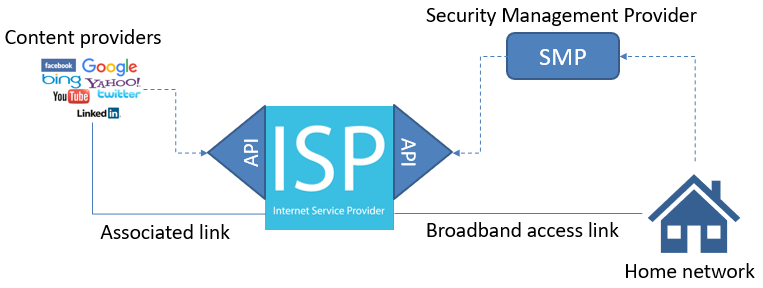


Figure ‎2‑5 High-profile architecture

# Security in IoT-based environments from both software and hardware standpoints

## Effect of IoT features on security and privacy

The number of IoT devices increases, therefore the communication between them becomes more complicated and leads to moderate human involvement. IoT devices progressively rely on smart devices with built in sensors and applications that support them. Most of them could also be inevitably guided by other multiple devices functions like using services like IFTTT (if this then that) which is a free web-based service to create chains of simple conditional statements, called applets [14], being recommended in numerous IoT application situations. The target device or the operation itself may not be effortlessly jeopardized, but hackers might efficiently manage to change other devices performances or the environment around, having an interdependence connection. Thus, this characteristic can be maliciously used to diminish the challenge of directly attacking the aimed devices and avoid the initial defense system. Usually, the researchers do not recognize the influence of interdependence behaviors on IoT security. Researchers regularly secure the device alone. Nevertheless, it is challenging to make a precise protective boundary of IoT devices or utilize static access control systems and authorize administration to them because of their interdependent nature. Besides, the supervision of many IoT devices handled by cloud platforms systems like Amazon Alexa [15], Ali [16], Samsung SmartThings [17], etc., which nowadays have acquired a considerable reputation within the smart home environment. Because the IoT device behaviors can be exchanged with different devices or environments, it is challenging to specify a precise series of detailed authorization standards for them. A typical issue in the authorization pattern of existing IoT platforms systems is the overprivilege [18].

### The Security Features of IoT

IoT security challenges can be classified using two cases, namely technological challenges and security challenges. The technological challenges are a result of the heterogeneous and ubiquitous character of IoT devices, whereas the security challenges are associated with the systems and functionalities that should be implemented to produce a secure network. Technological challenges are associated with wireless technologies, scalability, energy, and distributed nature, on the other hand, security challenges are concerned with the lack of the ability to ensure security by authentication, confidentiality, end-to-end security and integrity. Security should be implemented in IoT throughout the improvement and operational lifecycle of all IoT devices and hubs. It is important for the software running on all IoT devices to be authorized. Before anything else, when an IoT device is turned on, it should authenticate itself into the network, and afterwards to start collecting or transmitting any kind of data. Considering the IoT devices have restricted computation and memory skills, firewalling is an important factor for the IoT network to filter packets addressed to the devices. The updates and applications on the device should be installed in a way that the supplementary bandwidth is not utilized [19][20].

Also, IoT will meet a significant development in the automation area. To further support very autonomous mechanisms, IoT will have the abilities to configure, repair and coordinate itself. The automation expansion leads to a rise in the vulnerability of the systems. Because of automation, manual interaction will become extensively reduced. An automated monitoring security system will be vital with the rise of management frameworks capacity, as the personnel will not cope with handling all the incoming logs and data [21].

### Challenges with Security Principles

Balancing the end-user satisfaction, the costs and the implementation efforts with security is a must. There exists a certain give and take criteria between the level of safety and comfort provided by any solution. The level of confidentiality, integrity, availability and authentication required will consistently be determined using a sliding scale, having in mind the application, use case or environment. It is imperative to hit the precise balance between the expected security levels, and cost or even the practicability of implementation. For instance, a group of IoT devices like particular sensors, might require more processing power for advanced cryptographic transactions.

Obtaining an architecture that is regulated by various devices, applications and networks is also a challenge for the implementation of specified security principles and standards. The usage of regular security architectures would ultimately drive to higher product quality, faster innovation and integration, and a broader community allowing a better response to undesired intrusions when or if they arise [22].

## Security issues in IoT

Common problems in assessing security and privacy in industrial applications include [44][45]:

* **Lack of anti-virus protection**. Most simple access protection method involves the use of anti-virus protection, but in IIoT this can’t be used in case of devices directly connected to the Internet.
* **Lack of or improper authentication methods**. Each communication protocol must include secured passwords or advanced authentication steps
* Use of **obsolete operating systems** without security patches
* Use of **remote access management** protocols
* Use of **Wi-Fi networks** make them sensitive to dedicated cyber-attacks, such as the KRACK WPA2 vulnerability
* Use of **data logging** over WAN connections

### Software Standpoint

When studying IoT security, there are also essential terms that need to be taken into concern such as privacy, identity management, trust, End-to-End Security, authentication and access control [23][24]. Also, the types of equipment that are extensively utilized in automobiles, home lighting, security cameras, and other home-based sensors are controlled by different customers. These devices usually connected to the Internet, are generally cheaper, being mass-manufactured and having a weak software with poor firmware security.

#### Attacks on the cloud

Clouds are now free databases. Heading towards to cloud technology is more and more expected, and even IoT pursues this trend. Many IoT applications now provide connected platforms to the cloud such as Bolt, hardware and software that enable the user to build and control from anywhere IoT products and projects. It is indeed easier and more feasible to have a database on the cloud for IoT applications, to access data easily, wherever the devices are. Therefore, clouds are more subdued to numerous kinds of attacks, given their primary role. Many significant reports like the Internet of Fails, Internet of Crappy Things and FTC (Federal Trade Commission) technical reports have featured security in IoT spaces. By incorporating IoT in clouds, and given the existing vulnerabilities, the peril of accessing data that can be confidential is even more significant [25][26].

#### Wi-Fi security

The most used and universal wireless standard is Wireless Fidelity (Wi-Fi). Wi-Fi users can meet different kind of security threats, such as phishing websites. A Distributed Denial of Service (DDoS) attack [27] represents a combined effort to make an online service unavailable by submerging it with traffic from repetitive sources. They target a broad variety of essential resources, from banks to news websites, and present a significant challenge in making sure people can advertise and access valuable information. DDoS attacks can also happen on Wi-Fi and flood the network. Access is also crucial for Wi-Fi considering not everybody can connect to a Wi-Fi network, but only those having the password. The problem appears in the case when in IoT not all “objects” have a user interface or keyboard. For example, how could we write a password in a smart T-shirt that only contains a very tiny chip with the sensor? Besides, if the Wi-Fi network is not suitably secured, there is a chance that a connected object in a given system can access other objects in the same network. It is an omnipresent issue on the Internet nowadays and is undoubtedly a threat even for IoT security.

### Hardware Standpoint

#### End Devices and Sensors

Sensors and embedded devices around the world will continue to increase in numbers more and more. They will have IP addresses and will communicate with TCP protocols through protected applications, yet many will utilize their own or ad-hoc communication techniques, like the unreliable 802.11 or Bluetooth. The information taken from the devices will be available from the proxy server, which might be even a smartphone. The connection to that intermediary server allows the attacker the capacity to investigate or change a considerably larger measure of data than previously. To conserve privacy and accessibility, system users ought to investigate the registered data, transmitted by the devices, and to secure access as required. Eventually, the data amount will increase so much that will be too substantial for anyone to monitor, therefore more powerful security instruments should be created to approve protected information flow from devices.

#### Wearable Devices

Various personal-based wearable devices do not connect directly to the internet or a network but instead via mobile devices such as smartphones that function as a communication hub for the wearables. Besides, the necessity of a direct connection to the wearable devices allows some privacy security to potentially confidential information. Using RFID devices such as identification badges, credit cards, and passports may not currently be combined into the consumer-based IoT, their service as authentication of identity and location in the workplace can adequately fit into the future global IoT. For example, as one procedure through a physical plant or one’s home, it may be beneficial for the lighting, heating, ventilation, and air conditioning (HVAC) system, audio-visual systems, or other “things” in the workplace or home, to recognize one’s presence and adjust equally. For a home setting, one might evermore need the television to resume a video series with the window shades and lighting adjusted accordingly. Wearable devices gather vast amounts of personal data as well as data about the user conditions. Significant privacy concerns appear for health-related data from the use of medical devices and fitness applications. Privacy-sensitive information can be easily disclosed to third parties. Threats occur for enterprise perimeters. Data from wearable devices and different quantified self-technologies are emerging into research and clinical form medical tools.

##### Medical Wearable Devices

When discussing about the design of medical devices [28], great attention should be addressed to the selection of wireless technology, for example IEEE 802.11, Bluetooth, wireless medical telemetry service, wireless connection stability, wireless protection, and performance frequency with minimum interference in the operation band of other nearby radio frequency devices, taking in consideration not only the country in which the product is made, but as well in other countries where it is going to be used.

##### Patient Information Privacy

Even though most of the healthcare organizations do not contribute with enough resources to preserve security and privacy, there is no doubt that security and privacy play an essential role in MIoT - Medial Internet of Things. Patient data can be subdivided into two divisions: sensitive data and common records. Sensitive data, which is usually called patient privacy, comprises sexual orientation, sexual functioning, psychological status, contagious illness, potency status, genetics, drug addiction and identity characteristics. Most importantly, the sensitive data must not be exposed to unauthorized entities. Even if the data is hijacked, the information expressed should not be understandable by unauthorized users.

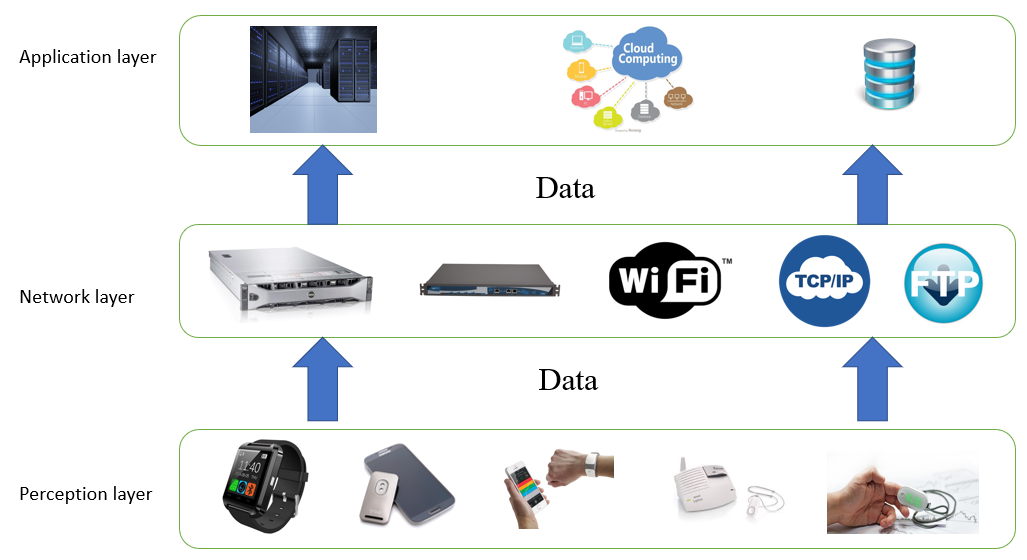


Figure ‎3‑1 Architecture regarding medical IoT

Usually, the MIoT architecture is composed of three layers [29]: the perception layer, the network layer, and the application layer, as described in figure Figure ‎3‑1. The main task of the perception layer is to assemble health care information with the different type of devices. The network layer, which is made of wired and wireless systems and middleware, operates and transfers the input gathered by the perception layer sustained by technological platforms. The application layer integrates the medical data sources to implement personalized medical services and comforts the definitive users’ needs, according to the genuine situation of the target community and the service demand.

#### Robotics

Modern robots used in the industry [30] can possibly modify the production mechanisms in the way computers have transformed the office workplace environment. Robots are used for their capabilities to accomplish tasks rapidly, accurately and continuously. They are relevant in various areas in the production industry and brought exceptional value to multiple construction mechanisms. For instance, the petrochemical industry uses robots to increase effectiveness and safety by also reducing the harmful impact towards the environment. In environments where is hazardous for people to work, robots come in handy because of their ability to provide maintenance and repairs. Still, there are some issues regarding trust and responsibility. The robots’ purposes within the organizational structure should also be considered. In the end, every shared system presents network layer vulnerabilities. Several robots autonomously function, whereas some may be controlled remotely. Robots have to be sufficiently predictable to function under complicated and active environments with increased confidence levels and still have the capacity to be firmly controlled or instead, to be stopped by the operator, so that the following generation of users and administrators to confide in autonomy. Keeping up this adaptability in the future framework will deliver adequate levels of trust in the activities performed by our robotic correspondents. The people's reaction to extended levels of autonomy has to be considered. Considering that robots do not have enough autonomy, then the administrator will linger on taking care of robots instead of their work. Likewise, another ability should advance for future administrators, in order to repair and preserve robots in their environments. The autonomous capacities primary advantages are to broaden and supplement people’s performances, not to fully substitute them. If robots have high autonomy levels, the awareness activities might decrease. Robots can enhance people’s speed, perception, ingenuity, resistance to tiredness. Several robots will include the capacity to investigate and carry samples and others will do more refined activities such as repairs and preservation. Mobile robots such as unmanned flying vehicles have been produced to function during a disaster, or just for examinations.

Nanobots represent a branch within robots’ field, being widely explored in the security and defense domains nowadays.

##### Nanobots

Nanobots represent a type of a little robot [30]. A nano-robot represents an artificial robot with the dimension of few micrometers or less, comprised from nanoscopic elements with distinctive sizes in the interval from 1 to 100 nm. A nanobot displayed the ability to travel freely through the hole human body circulatory system. In the future, these nanobots could be utilized in production systems, as in the provisioning of a microscopic view towards the situations crucial to specific bio-pharmaceutical or nuclear facilities. The idea of studying the state of fluid suspension with entire groups of nanobots could be explained in the bloodstream. A nanobot in a vein has shown the ability to feel the metabolic sequence of the family of cells fed by the vein itself, therefore examining the cells restrained within a given length of the tube. Each nanobot is a self-propelled device, taking energy from the environment, being able to identify and anchor to the elements within their process. They can sense membranes and consequently recognize the state of health of its environment. They also may be applied to collect the information, to transmit it to the central unit, and ultimately, take actions that might affect the overall process situations. Within an entire group of nanobots, each bot holds particular chemicals to be released for detection by other nanobots. This could also be used in a production facility to carry a message from one location to the other.

It is a difficult matter to ensure that nanobots and nanobot groups are working securely. Nanobots are by definition tiny and are therefore very challenging to monitor for unique malicious behaviors, especially if a massive group of nanobots is transmitted. If nanobots alone are programmed with software, how may someone scan the nanobot’s operating code for malware? If nanobot groups are programmed with chemical means, would there be a means to assure that the use and control of the swarm not be taken over by a malicious entity, in the same manner, that bacteria and viruses affect the biological receptors? How the nanobot group will be supported and monitored? How nanobots are disposed, when they reach their end of life? As with other features of innovative IoT devices, nanobot systems provide great utility but have not been yet analyzed or developed for security and safety.

### Embedded Secure Element (eSE)

The eSE (embedded Secure Element) is **a tamper-proof chip** available in different sizes and designs, **embedded in any mobile device**, **wearable or IoT**. It ensures the data is stored in a safe place and information is given to only authorized applications and people. It is like a personal ID for the end-user and for the device itself.

The eSE is multi-applicative and allows to secure a wide range of applications in any type of device and in various use cases: payment, couponing, transport, access control, ticketing, corporate, cloud computing, e-government. Depending on the device, eSE functionalities can vary, particularly the remote and secure way to retrieve data, secure connectivity, strong user authentication, device integrity, etc.

On the field of Security, the eSE is certified by major governments (French National Office for Information Security ANSSI, German Federal Office for Information Security BSI, …) and payment schemes (EMVCo, Visacard, Mastercard, AMEX, …).

#### Way forward to crypto agility

Resilience will be the main security challenge for the coming decade. Our world relies on secure digital cryptography. Secure doesn’t mean unbreakable forever. For the matter of comparison, average lifespan of consumer electronics and tech devices is evaluated between 5 to 15 years, ID documents lifetime is extended to 10 years by governments, security certificates are delivered with a validity date of 5 years, and it’s hard to name a respected cryptographic algorithm that hasn’t fallen in recent years.

Crypto-agility becomes the key challenge. Preparing for moving from one implementation to another without having to re-do or re-write everything, could it be patches, mitigations or algorithm replacements.

Quantum computers are coming. It is foreseeable that the main asymmetric algorithms used in cryptography today to protect critical infrastructure, software update, payment mechanisms, media streaming, IoT devices, connected cars, government or financial secrets or documents will no longer be safe. Then post-quantum “crypto agility” seems to be the future. For US, the National Institute of Standards and Technology (NIST) has initiated a process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms [56].

Several recognized security instances have provided their recommendations (German Federal Office for Information Security BSI [54], Internet Engineering Task Force IETF [55], …)

## Security Threats

Security threats facing IP protocol related devices have been well analyzed and discussed in several documents including Hypertext Transfer Protocol (HTTP) over Transport Layer Security (TLS) (HTTPS) [[57]](https://tools.ietf.org/id/draft-irtf-t2trg-iot-seccons-14.html#RFC2818), Constrained Application Protocol (COAP) [[58]](https://tools.ietf.org/id/draft-irtf-t2trg-iot-seccons-14.html#RFC7252), IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) [[59]](https://tools.ietf.org/id/draft-irtf-t2trg-iot-seccons-14.html#RFC4919), Access Node Control Protocol (ANCP) [[60]](https://tools.ietf.org/id/draft-irtf-t2trg-iot-seccons-14.html#RFC5713), Domain Name System (DNS) [[61]](https://tools.ietf.org/id/draft-irtf-t2trg-iot-seccons-14.html#RFC3833), IPv6 Neighbor Discovery (ND) [[62]](https://tools.ietf.org/id/draft-irtf-t2trg-iot-seccons-14.html#RFC3756), and Protocol for Carrying Authentication and Network Access (PANA) [[63]](https://tools.ietf.org/id/draft-irtf-t2trg-iot-seccons-14.html#RFC4016). Throughout this section, we focus on the main threats that could compromise an individual smart device as part of its network and eventually the network as a whole. Some of these threats, as discussed in previous sections, might go beyond the scope of Internet protocols. The following threats are listed in [65]:

1. **Software/Code Vulnerably**: Nodes which are part of the Internet of Things rely on software that might contain severe bugs and/or bad design choices. This makes the smart devices vulnerable to many different types of attacks, depending on the criticality of the bugs, e.g., buffer overflows or lack of authentication. This can be considered as one of the most important security threats. The large-scale distributed denial-of-service (DDoS) attack, popularly known as the Mirai botnet, was caused by things that had well-known or easy-to-guess passwords for configuration.
2. **Privacy threat**: The tracking of a thing’s location and usage may pose a privacy risk to people around it. For instance, an attacker can infer privacy sensitive information from the data gathered and communicated by individual things. Such information may subsequently be sold to interested parties for marketing purposes and targeted advertising. In extreme cases, such information might be used to track dissidents in oppressive regimes. Unlawful surveillance and interception of traffic to/from a thing by intelligence agencies is also a privacy threat.
3. **Cloning risk**: During the manufacturing process of a thing, an untrusted factory can easily clone the physical characteristics, firmware/software, or security configuration of the thing. Deployed things might also be compromised, and their software reverse engineered allowing for cloning or software modifications. Such a cloned thing may be sold at a cheaper price in the market, and yet can function normally as a genuine thing. For example, two cloned devices can still be associated and work with each other. In the worst-case scenario, a cloned device can be used to control a genuine device or perform an attack. One should note here, that an untrusted factory may also change functionality of the cloned thing, resulting in degraded functionality with respect to the genuine thing (thereby, inflicting potential damage to the reputation of the original thing manufacturer). Moreover, additional functionality can be introduced in the cloned thing, an example of such functionality is a backdoor.
4. **Malicious substitution**: During the installation of a thing, a genuine thing may be substituted with a similar variant (of lower quality) without being detected. The main motivation may be cost savings, where the installation of lower-quality things (for example, non-certified products) may significantly reduce the installation and operational costs. The installers can subsequently resell the genuine things to gain further financial benefits. Another motivation may be to inflict damage to the reputation of a competitor’s offerings.
5. **Eavesdropping attack**: During the commissioning of a thing into a network, it may be susceptible to eavesdropping, especially if operational keying materials, security parameters, or configuration settings, are exchanged in clear using a wireless medium or if used cryptographic algorithms are not suitable for the envisioned lifetime of the device and the system. After obtaining the keying material, the attacker might be able to recover the secret keys established between the communicating entities, thereby compromising the authenticity and confidentiality of the communication channel, as well as the authenticity of commands and other traffic exchanged over this communication channel. When the network is in operation, T2T communication may be eavesdropped upon if the communication channel is not sufficiently protected or in the event of session key compromise due to protocol weaknesses or a long period of usage without key renewal or updates. Messages can also be recorded and processed offline at a later time.
6. **Man-in-the-middle attack**: Both the commissioning phase and operational phases may also be vulnerable to man-in-the-middle attacks. For example, when keying material between communicating entities is exchanged in the clear and the security of the key establishment protocol depends on the tacit assumption that no third party can eavesdrop during the execution of this protocol. Additionally, device authentication or device authorization may be non-trivial, or may need support of a human decision process, since things usually do not have a-priori knowledge about each other and cannot always differentiate friends and foes via completely automated mechanisms.
7. **Firmware attacks**: When a thing is in operation or maintenance phase, its firmware or software may be updated to allow for new functionality or new features. An attacker may be able to exploit such a firmware upgrade by replacing the thing’s software with malicious software, thereby influencing the operational behavior of the thing. For example, an attacker could add a piece of malicious code to the firmware that will cause it to periodically report the energy usage of the lamp to a data repository for analysis. Similarly, devices whose software has not been properly maintained and updated might contain vulnerabilities that might be exploited by attackers to replace the firmware on the device.
8. **Extraction of private information**: IoT devices (such as sensors, actuators, etc.) are often physically unprotected in their ambient environment and they could easily be captured by an attacker. An attacker with physical access may then attempt to extract private information such as keys (for example, device’s key, private-key, group key), sensed data (for example, healthcare status of a user), configuration parameters (for example, the Wi-Fi key), or proprietary algorithms (for example, algorithm performing some data analytics task). Even when the data originating from a thing is encrypted, attackers can perform traffic analysis to deduce meaningful information which might compromise the privacy of the thing’s owner and/or user.
9. **Routing attack**: Routing information in IoT networks can be spoofed, altered, or replayed, in order to create routing loops, attract/repel network traffic, extend/shorten source routes, etc. Other relevant routing attacks include 1) Sinkhole attack (or blackhole attack), where an attacker declares himself to have a high-quality route/path to the base station, thus allowing him to do manipulate all packets passing through it. 2) Selective forwarding, where an attacker may selectively forward packets or simply drop a packet. 3) Wormhole attack, where an attacker may record packets at one location in the network and tunnel them to another location, thereby influencing perceived network behavior and potentially distorting statistics, thus greatly impacting the functionality of routing. 4) Sybil attack, whereby an attacker presents multiple identities to other things in the network.
10. **Elevation of privilege**: An attacker with low privileges can misuse additional flaws in the implemented authentication and authorization mechanisms of a thing to gain more privileged access to the thing and its data.
11. **Denial-of-Service (DoS) attack**: IoT nodes often have very limited memory and computation capabilities. Therefore, these constrained devices are vulnerable to resource exhaustion attacks, where attackers can continuously send requests targeting specific devices in order to deplete their already limited resources. This is especially dangerous in the IoT networks since an attacker might be located in the backend and target resource-constrained devices that are part of a constrained node network [64]. DoS attack can also be launched by physically jamming the communication channel. Network availability can also be disrupted by flooding the network with a large number of packets. On the other hand, things compromised by attackers can be used to disrupt the operation of other networks or systems by means of a Distributed DoS (DDoS) attack.

# User data management in IoT-based environment

Cloud Computing is an important research area due to the ability to reduce costs and to provide various types of facilities for users. Nowadays, the technology is increasingly based on the concepts of storage, connectivity, virtualization, and processing power. Since Cloud Computing stored the data in an open environment, security has become the main concern for the implementation of Cloud.

Information security is essential to protecting data from the users' systems and application. With the transition to Cloud Computing, the traditional methods of securing data are challenged by new cloud-based architectures. The elasticity, the unique physical and logical architectures require new strategies for the data security. In many Cloud deployments, data is transferred to external, or even public, environments, in ways which were unthinkable a few years ago.

Managing the information is a challenge for all organizations, even those which are not engaged in Cloud Computing. The first step is to control the internal data and the Cloud migrations, and then to secure the diffused information from applications and services. For data security and information management, new strategies and technical architectures are needed. Fortunately, the required tools and techniques are available for users, and cloud transition creates opportunities to secure data in traditional infrastructure.

## Cloud Information Architectures

Cloud Information architectures have the same diversity as the cloud architectures themselves.

### Infrastructure as a Service (IaaS)

IaaS, for public or private Cloud, usually includes the following storage options:

* Raw storage: Includes the physical media where data is stored and can be mapped in individual cloud configurations for direct access;
* Volume storage: Includes the volumes attached to IaaS instances, often under the form of a virtual hard drive. These usually utilize data dispersion to bolster flexibility and privacy;
* Object storage: Is sometimes delivered as file storage and is more like to a file share accessed via API or web interface rather than a virtual hard drive;
* Content Delivery Network: The content, firstly stored in object storage, is then distributed to multiple geographically nodes to improve consumption speeds.

### Platform as a service

Platform as a Service (PaaS) provides a variety of storage options:

* Database as a Service: A database is directly used as a service. Users consume the database via APIs or SQL calls, depending on the offer. Each customers’ data is separated and isolated from the others. The database can be relational, flat or have any other structure;
* Hadoop/MapReduce/Big Data as a Service: Many Big Data applications (e.g. Hadoop) can be offered as a Cloud Platform. Data is usually stored in Object Storage, or in any file system and needs to be close to the processing environment, so, if it is required, the data can be moved temporarily for processing;
* Application Storage: Includes every storage option which was built into a PaaS application platform and consumable via APIs which are not included in others storage categories.

### Software as a Service

Software as a Service (SaaS) uses a wide range of storage and consumption models. SaaS storage is accessed via a web-based user interface for both client or server application. SaaS can provide:

* Information Storage and Management: Data enters into the system via the web interface and is stored within the SaaS application, which is typically a back-end database;
* Content/File Storage: The content is stored within the SaaS application and is accessible via the web-based interface.

### Data Dispersion

Data Dispersion is a standard technique used to improve data security, without using the encryption mechanism. This type of algorithms is capable of providing high availability and assurance for the data stored in Cloud using data fragmentation and are common in many Cloud platforms.

In a fragmentation scheme, a file, f, is split into n fragments, signed and distributed to n remote servers. Then the user can reconstruct the file by accessing m arbitrary chosen fragments. The fragmentation mechanism is also used for storing long-living data in Cloud with high assurance.

Data security can be enhanced if the fragmentation and encryption mechanism are used together. This way, an adversary firstly needs to compromise m Cloud nodes to retrieve m fragments of the file f and then to break the encryption mechanism.

## Information Management

Information management includes the policies and processes for using and governing the usage of the information.

### The Data Security Lifecycle

Information Lifecycle Management is a mature field which doesn't map with security professionals' needs, different from Information Lifecycle Management and reflecting the diverse needs of the security audience.

Data Security Lifecycle includes six phases as presented in figure Figure ‎4‑1, starting with the creation of data and finishing with destruction. Although, it is shown as a linear progression, once created, data can be transferred through phases without any restriction and may not pass through all stages (for example, not all data is eventually destroyed).

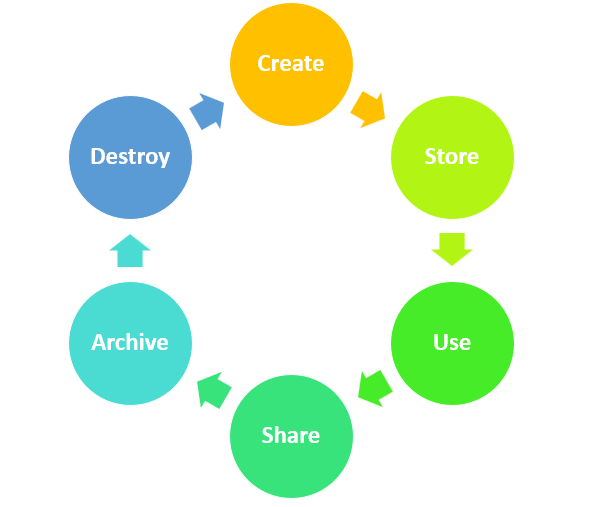


Figure ‎4‑1 Cloud computing data life cycle

1. Create: Creation can be defined as the generation of new digital content, or as the alteration/updating of the material so that the users can fill in personal data, or the data can be gathered from environmental sensors;
2. Store: Storing means committing the digital data to a storage repository, and it usually coincides with the act of creation - Graphite at this point; the user needs to ensure that the security controls have been implemented and the data is protected;
3. Use: During this stage, the information is viewed, processed or used in different activities. Data usage can be a product or a service, depending on the user’s offering. - generate graphs;
4. Share: Data is continuously shared between different types of users. It moves among a variety of public and private storage locations or other operating environments;
5. Archive: At this point, the data moves from an active environment and enters long-term storage;
6. Destroy: If the information is no longer needed, it must be adequately destroyed using physical or digital means (e.g. crypto shredding).

#### Locations and access

Data Lifecycle represents all the stages of data throughout its life but doesn’t address its location or how is accessed.

Locations can be illustrated by thinking of the Lifecycle as a series of smaller lifecycles running in different operating environments. In any phase, the data can move into, between or out of these environments. Due to all potential issues, it is essential to understand both the physical and logical locations of data.

Once established to the place where the data will be saved and how it will move, the user will need to know how its data is accessed.

There are two factors which influence how data is accessed:

1. Who can access the data?
2. How can information be obtained (device or channel)?

Today's data can be accessed from all sorts of devices which have different security characteristics and may use various types of applications or clients.

#### Actors, Functions and Controls

This paragraph identifies actors (people or systems) which can perform functions with the data in a particular location.

There are three functions which can be performed with a given data by an entity (app., person, or system/process, in contrast to the access device):

* Access: View/access the data which includes creating, copying, transferring, dissemination or other activity where information is exchanged;
* Process: Accomplish a transaction on the information: update, use for processing a transaction, etc.;
* Store: Store the data (in a file, in a repository, etc.).

A control restriction means that are allowed only several actions from a list of possible activities.

### Information Governance

Information governance includes all the policies and procedures for managing the information usage and consists of the following key features:

* Information Classification: Includes the description of the relevant information categories. The purpose is to define all high-level classes to determine the needed security controls;
* Information Management Policies: Define the allowed activities for different information types;
* Location and Jurisdictional Policy: Store all geographical places where data can be located and have regulatory and legal ramifications;
* Authorizations: Define which kind of information can be accessed from which type of users/employees;
* Ownership: Defines who is ultimately responsible for the data;
* Custodianship: Defines who is responsible for the management of the information at the request of the owner.

## Data Security

Data Security includes all specific technologies and controls needed to enforce information management.

This topic can be divided into three sections: to cover the detection and prevention of the migration of data to Cloud, the protection of data in the transfer between Cloud and different environments and the security of data once is stored in Cloud.

### Internal Data Migration

Before data can migrate to Cloud, it needs to be pulled from the place (depository, database, file, etc.) where is saved. Database Activity Migration will detect any activity which may mean a migration (e.g. when an administrator or other user replicates a database or pulls a data set).

### Movement to Cloud

The transfer from the enterprise to Cloud can be detected with a combination of URL (Uniform Resource Locator) filtering and Data Loss Prevention.

The URL filtering allows the user to monitor and access the connection to Cloud services. The administrative interfaces for these devices use different addresses than the consumption side it should be detected if someone is accessing an admin console or if a user is accessing an application which is already hosted with the provider.

For increasing the granularity, the users should use Data Loss Prevention (DLP) which has the main advantage that the DLP tools look at the transmitted data, not just at the destination. Alerts can be generated based on the classification of the data. For example, a private data set can be allowed to go to an approved Cloud service, but it can be blocked to migrate towards an unauthorized service.

### Secure Data Transfer within/to the Cloud

Throughout different service models or in both public and private cloud deployments, it is essential to protect data in transit.

This includes:

* The transition of data from the traditional infrastructure to Cloud providers, including public/private, internal/external and other permutations;
* The transition between Cloud providers;
* The change between instances within a given Cloud.

There are three options:

* Link/Network Encryption: Standard network encryption techniques include SSL, VPNs, and SSH;
* Client/Application Encryption: Encryption is used before being sent across the network, and it includes local client encryption or encryption integrated into applications;
* Proxy-Based Encryption: The data is transmitted to a proxy appliance or server for encoding before sending further on the network, and it’s a preferred option for integration into legacy applications.

#### Object Storage Encoding

Object storage encoding secures multiple types of the same risks, like volume storage which also allows the user to implement a VPS (Virtual Private Storage), so he can use a public shared infrastructure while protecting the data.

* Folder/File encoding and Enterprise Digital Rights Management: Before placing in the object storage, it uses standard file/folder encryption tools or EDRM (Electronic Discovery Reference Model);
* Client/Application encryption: It’s needed when object storage is used as the back-end for an application;
* Proxy encryption: Before sending the data to the object storage, data needs to be passed through an encryption proxy.

#### PaaS Encryption

Potential options for PaaS encryptions:

* Application/Client encryption: Data is encrypted in the PaaS application while is getting into the platform;
* Database encoding: Data is encoded in the database utilizing the encryption provided by the platform;
* Proxy encryption: Before sending the data to the platform, data needs to be passed through an encryption proxy;
* Other: Addition options may include external encryption services, APIs or other variations.

#### SaaS Encryption

SaaS providers are recommended to use per-customer keys to improve multi-tenancy isolation. SaaS consumers have the following options:

* Provider-managed encryption: In the SaaS application, the data is encrypted and managed by the provider;
* Proxy encryption: Data is encrypted in the database using the encryption provided by the SaaS application.

Encryption operations may use a shared key or public/private key pairs and extensive PKI/PKO (Public Key Infrastructure/Operations) structures.

#### Data Loss Prevention

Data Loss Prevention (DLP) products are based on central policies which detect potential data breaches and prevents them by monitoring and identifying sensitive data with the following options:

* Dedicated appliance/server: Includes the standard hardware placed within different Cloud segments or at a network blockage between the Internet and the Cloud;
* Virtual appliance;
* Endpoint agent;
* Hypervisor-agent: The DLP is embedded/accessed at the hypervisor level;
* DLP SaaS: DLP is offered as a standalone service (typically content discovery) or is integrated into a Cloud service.

#### Monitoring database’s activities and files

Database activity monitoring (DAM) may be defined as a database security technology which captures and records all SQL activities (SQL) in real-time, including database administrator activity and can generate alerts on policy violations.

#### Application Security

Most of the data exposures are the results of attacks at the application layer.

#### Privacy Preserving storage

Many cloud-based storage systems require a participant authentication (cloud user and/or CSP) to establish trusted relations, for one or two endpoints of the communication. Cryptographic certificates can provide sufficient security for many purposes, but they usually don’t satisfy confidentiality because they are connected with the identity of the cloud user. The usage of these certificates is to expose the integrity of the holder to the party requesting authentication.

Electronic Health Record is just a scenario where the usage of the cryptographic certificates unnecessarily reveals the identity of the holder.

Many technologies have been developed to build systems in different ways to save and protect the privacy of their holder. These attribute-based credentials are issued like any other ordinary cryptographic credentials with a digital (secret) signature key. Any application or system which works with Digital Rights Management (DRM) protected data must be able to implement and interpret the rights and also means to integrate the key management system.

There are two broad categories of DRM:

* Consumer DRM (C-DRM);
* Enterprise DRM (E-DRM).

Both types share the same DRM technology, but there are some significant differences, shown in the following table:

Table ‎4‑1 Consumer DRM vs. Enterprise DRM

|  |  |  |
| --- | --- | --- |
|  | Enterprise DRM | Consumer DRM |
| Authentication | Two-factor authentication | Simple authentication |
| ACL (Access control list) | Flexibility required | Not necessary |
| Auditing/Tracing | Required | Privacy issues |
| Connectivity | Existing ECM | Payment gateway, home networks, etc. |

# User Data Protection and Privacy Preservation

## Privacy and User Data Protection Approaches

### User privacy concerns

Privacy protection is a step further in user data protection mechanisms, which relies mainly on security mechanisms such as authentication, authorization and encryption, which ensure data integrity and confidentiality. Privacy protection aims at enabling users to take full control of their own personal data, which means to have a right to consent/deny sharing them with any external entity, to be informed about all the processes the data are subject to and the conclusions drawn from them (inferences, cross-analysis with other data, etc.), to be able to retract the consent for any reason, and to delete definitely the data collected by the connected objects.

User data privacy protection has been tackled in different works and contexts such that user data protection on the web, data anonymization, data minimization and shelf life, etc. We detail in this section the main approaches and solutions introduced in these contexts.

Privacy protection can be defined in different ways. General privacy is defined as the “right to be left alone” by Warren and Brandeis’s (1890) introduced in the late of 19th century in the United States during the large spread of the press, where privacy concerns are mostly about reputation. Nowadays, the concept of privacy protection is more challenged by the growth of connected objects, which collect and communicate personal data to external entities and the boom of data analysis techniques (called big data). Privacy concerns have been considered then in direct marketing, Internet and e-commerce, data mining and profiling (personalization), monitoring and surveillance, communication (e-mail, SMS, IM, phone call, etc.), ubiquitous computing (IoT based applications, wearable sensors, smart cities, smart grids, trackers, etc.), Web 2.0 (social networks) [58][54][53], and more recently in cloud computing. Different techniques have been developed in the domain to ensure privacy in the context of IoT [70][66], but as stated in [70], “privacy requirement in IoT is currently only partially covered”. There is a real need for privacy policies definition model capable to deal with the scalability and the high dynamicity which characterize IoT environments.

### User Data Protection and Privacy preservation methods in IoT applications

IoT-based applications are two-edged sword. On one hand, they allow developing public and private infrastructures that provide good solutions for improve people’s everyday life (healthcare, transportation facilities, home automation, public administrations, etc.). On the other hand, such applications and facilities disclose too many information about users that could threat and undermine privacy, equality, trust, and individual choice, if they are not actually designed, implemented and governed in appropriate ways.

Several platforms for personal data protection have been proposed in diverse contexts. For instance, [[72](#LyXCite-Serrano_Alvarado2013)] introduces “Privacy-Lookout” as a framework based on a personal linked data view of individuals that organize and enrich the meta-information of their personal data existing in the web. It permits people to be on the lookout for any infringement of their personal data privacy. However, it does not allow individuals to specify globally their data privacy policies.

In [[69](#LyXCite-Montjoye2012)], the authors introduced “openPDS” for open-source Personal Data Store, which is compliant with some US recommendation like the US Consumer Privacy Bill of Rights. It aims at enabling users to collect, store, and give fine-grained access to their data in the cloud while protecting their privacy. The authors raised the need for the development of techniques to detect breaches and attacks, by auditing the outgoing data to verify that no unexpected data is escaping the boundaries of one’s PDS. In [90], the authors proposed a combination of (i) a self-controlling and self-monitoring object called “SafeShare” in order to encapsulate user data and access policies, and (ii) and encryption methods (Ciphertext-Policy Attribute-Based Encryption CP- ABE) and ELGamal encryption schemes to secure data sharing and collaboration in the cloud. The drawback of the approach lies in its time consuming due to the encryption/decryption functions, raising a scalability issue of the available solutions. Previous approaches to mitigate the threats to user data have been also developed. For instance, it is possible to make use of “Trusted Platform Module” (TPM), introduced by [87] to ensure the integrity of the connected objects, and cryptography solutions to secure communication channels amongst IoT objects [88][73].

Vincent et al in [74] proposed an ontology-based firewall to protect the user’s digital identity and personal data. A firewall makes decisions about allowing or denying the access to data to connections according to a set of rules describing the semantics of the rules and the external entities using them.

Moreover, there are new approaches based on machine learning for protecting data collected from sensors against sensitive inferences [84][85]. The inferences in these cases refer to the application of the pre-trained deep model on input to obtain the output. The approaches are defined over time-series data to predict non-sensitive activities, while altering the inferences of sensitive attributes such as gender, age, weight, height, etc. These approaches need to be provided with the set of non-sensitive activities and the set of sensitive data to protect. Furthermore, they alter the data so as it becomes impossible for a deep learning approaches to train a good enough model for predictions.

### Data anonymization methods

Data anonymization encompasses diverse techniques such as k -anonymity, pseudo anonymity, data aggregation, l-diversity, etc. It aims at preventing from re-identification of individuals by linking several micro-datasets published by diverse companies and organizations, as non-aggregated data (tables of medical, voter registration, census, and customer data, etc.), but each micro dataset is itself perfectly anonymized by removing any identifying information like name, social security number, phone number, etc. [75].

For instance, gender, birthday and 5-digit zip code can uniquely identify 87% of the population of the USA [76]. Thus, the approach needs to identify a set of attributes, which combined with an external data source, they allow identifying a unique tuple in the dataset. These attributes are called quasi-identifiers. This kind of data combination to identify individuals is called linking attack. To face this attack, the k -anonymity privacy definition has been proposed by [77][78]. The authors stipulate that “a table satisfies k -anonymity if every record in the table is undistinguishable from at least k-1 other records”.

The k-anonymity approach does not really protect user privacy since it is subject to at least two attacks, namely homogeneity attack and background knowledge attack [75]. Both attacks are possible when (i) tuples of a considered k-anonymity table can be gathered by groups over their sensitive attributes (for instance, health condition is a sensitive attribute in an anonymized health records tables), such as each group contains tuples having the same value for sensitive attributes and (ii) the attacker has some knowledge about the individuals targeted (knowledge which is actually easy to obtain from social networks, personal blogs and website, etc.). To overcome this drawback, the l-diversity approach [75] has been introduced which combines the k-anonymity with the requirement that the values of sensitive attributes are well represented in each group.

Even though the set of answers contains more than one tuple, it is still easy to threat user privacy [79] since the research space has been dramatically reduced due to the lack of diversity in k-anonym tables. The approaches summarized here have been designed for datasets, which are structured as databases, in which data is described as tuples or records with attributes and values. In the case of IoT environments, data collected from connected objects are diverse, massive, and heterogeneous. The data is not supposed to be leaked out publicly even in anonymous ways, and their exploitation and sharing should obey to private protection policies defining a trustworthy relationship between the user and application developers and service providers.

### Data Minimization and Data Shelf Life

Principles of data minimization and shelf life have been widely adopted by public authority regulations in Europe and the US and have been also presented as main principles of the Privacy by design approach. Data minimization refers to the fact that an application should not acquire more data than what it needs to provide a service. Data shelf life means that once the application is done with data acquired, it should delete them definitely. To the best of our knowledge, there is no implementation of these principles.

Another means for data minimization/anonymization is data aggregation. For instance, instead of sharing personal data of all the people having the seasonal flu, the system shares only the percentage of sick people in a given area. There are many existing works on preserving user privacy in aggregation data such as [67] in smart cities, [80] in mobile healthcare networks, and [81] in smart grids to name a few. It would be worthy to consider data aggregation in our platform to enable users to define different ways to share their data with service providers or any other third party.

Wireless sensor networks (WSNs) are nowadays considered as an important part of the Internet of Things (IoT). In these networks, data aggregation plays an essential role in energy preservation. However, WSNs are usually deployed in hostile and unattended environments in which the confidentiality and integrity security services are widely desired. Traditional secure aggregation protocols use hop-by-hop encryption, in which sensor nodes encrypt the captured data and send the cipher text to the aggregator node; the aggregator node decrypts, performs the aggregation function, and then sends the encryption of the result to the upper aggregator node. Therefore, while these data aggregation protocols improve the bandwidth and energy utilization of the network, and especially allow a simpler implementation of aggregation functions (Maximum, Minimum, Average, etc.), they incur not only a high computation overhead but also delay (due to encryption/decryption effort). Besides, the aggregator nodes can access to the plaintext data, so the end-to-end confidentiality is not provided which is mandatory, especially for military applications. Recently, homomorphic encryptions have been applied to conceal sensitive information during aggregation such that algebraic operations are done directly on cipher texts without decryption. The main benefit is that they offer the end-to-end data confidentiality and they do not require expensive computation at aggregator nodes since no encryption and decryption are performed. However, existing solutions either incur a considerable overhead or have limited applicability to certain types of aggregate queries. Therefore, the development of efficient schemes with stronger security becomes primordial.

The biggest challenge in data protection is maintaining secure people’s privacy as well as their personal information while using the data.

### Big Data and privacy

Sensors of the IoT, social media, communications, all have in common the need for privacy. Human activity leaves digital tracks which can be collected and stored by someone. All this data which came from several sources and in different formats, formed the Big Data (9.5 billion petabytes in 2015).

While big data are precious in many fields like data science or communication [36] (Facebook, Linkedin), it can also threaten the privacy of the user by collecting private data. Usually, to receive this data, the service provider offers a free service.

Personal data are protected by some principles (Art. 29 Data Protection Working party, new General Data Protection Regulation). Potential conflicts between these principles and the data collected may occur. When this happens, they are two ways of thinking. Either privacy must be minimized to avoid hindering technology development, or the collection must be minimized. Nihilists people think that privacy must be sacrificed, contrary to Fundamentalists people who believe that privacy is valuable even if the data becomes useless.

Data anonymization may be a possible way to overcome the conflict between big data and privacy.

## User Data Protection Tools

### Personal Information Management System

Some kind of tools can help users to manage their personal information, they are called Personal Information Management System (PIMS). PIMS is part of a relationship of trust between individuals and organizations. Instead of a system based on data capture by organizations unidirectionally or by a third-party to adapt services to its users, PIMS has a human-centered approach, where the user exploits his own data and manages their sharing with organizations. Benefits to the user are a takeover of his data, which implies economic choice or a better behavior knowledge.

**PIMS** are system which aim to give more control to persons over their personal data, according to the following aspects: the storage of data, their organization and management, the chosen share. More precisely, a personal data can be created by the person or provided by an external source like a private or public company that give back the data. Then data accessible by the system can be organized and managed for consultation, some of them can be updated or deleted. By sharing data, anonymously or only needed, the person exploits them using applications and third-party services for a better knowledge of his behaviour and way of consuming, make decision easier, to share individual or societal wishes that contribute to the production of collective knowledge …

A private or public company may interface with PIMS to provide personal data or to exploit data shared by the person. By choosing to give back personal data, companies or administrations engage into an interaction process toward their customers or citizens that enhances trust. With third-party services that processing data, private or public companies can respond, anticipate and suggest solutions closer to personal needs and desires of customers [38].

**Mes Infos** project: MesInfos [39] is a project led by the Fing association. This is a personal data disclosure experiment where several large companies (network operators, banks, retailers, insurers…) have agreed to share with a panel of customers the personal data that they held about them. The aim is to explore, in an agile and practical manner, the value that individuals could derive from being empowered with their own data according to different use cases: value-based living, contribution to research and collective endeavors, control of data, decisions and action, life experience...

**Cozy** is a dashboard application centralizing personal data that come from several large companies which have agreed to share witch customers. Users can retrieve their data with third-party services, manage and organize their data, files and contacts, add extension services such as tracking daily expenses and visualize statistics about expenses items.

**Solid** [40] is a project taking place at MIT and led by Tim Berners-Lee, inventor of the World Wide Web, that proposes tools for building decentralized social application like a collaborative read-write space. Owner content is decoupled from applications, so that only the data is persistent for the user, who can then switch between applications.

**StackSync** by Tissat is a unified digital locker for our personal data offering three key services: Storage, Synchronization and Sharing. It provides redundant and trustworthy cloud data storage for our information flows irrespective of their type. Also, it provides syncing and file exploring capabilities in different heterogeneous platforms and devices. And finally, it offers fine-grained information sharing to third-parties (users and applications). This is an open source product.

**CityZeen**‘s founder is coming from France, is also involved with FING which is an interesting organization promoting from 2012 an extension of PIMS movement. Canada was the worldwide championship in terms of privacy for Smart Grid so CityZeen is taking a very true engagement with Personal Information, acting in other R&D projects in Europe and America. CityZeen counts on the support of National Research Council and Private Commissioner who created Privacy by Design. Citizeen is a platform which linked persons and their government for what they need from their city, for example, parking, utilities, transportation, air pollution, waste traffic jams… The administration gets faster the desires of its citizens than the traditional administration model, information obtained is more accurate because given by persons

**Maidis** has strong expertise in clinical and personal data management in the healthcare domain by using several encoding standard systems and ontologies in compliancy with messaging systems such as HL7. The first innovations that Maidis will bring to the project is the unification of personal information and the provision of suitable data mining module to allow better management and interpretation of personal information into meaningful meta data concerning user behaviors, profiles and contexts. Linking personal information with health records in order to activate the self-management of healthcare through SaaS portals is another innovation that is strongly requested and valuable for e-Health/m-Health health markets. The resulting technology will be an SAAS Patient Repository which is centred on Privacy & Security, Users Profiles and Context of Personal Information Collection.

**Midata** [41] is a self-data project about consumers-centered approach, and not users-centered approach, carried by the British government and several large companies, which propose a term of service around fundamental points:

* consumer can recover his data safely
* consumer data demand must be addressed promptly
* consumer is free to process and share his data
* consumer will be accompanied in their empowerment with their data by companies
* consumer will be informed of the data collection and their meaning
* companies should not restrict data reuse
* terms, formats and data between organizations must be standardized as much as possible
* data are given back in open standards and are machine readable
* decision-making and conduct of specific activities are the meaning given to the data

## User Data Protection Regulations

### US versus Europe regulation for user privacy protection

It is worth noticing that public authorities in many regions in the world (Europe, US, Japan, Brazil, etc.) have considered user privacy protection along with the large adoption and development of Information and Communication Technologies (ICT). We limit our presentation to European and US standards to shed the light on the obligation in terms of security and user privacy requirements any application and/or device providers and manufacturers should respect towards the users.

Public authorities in Europe and USA have launched many working groups about personal data protection encompassing both data and user privacy protections. A large overview of these regulations has been carried out in [82] in which the authors have distinguished the main difference between the approaches pursued by both EU and USA. Mainly, US authorities try to protect people from government privacy violating activities, while the European approach places an affirmative duty on government to safeguard individual privacy (from any threats and violation from a third-party entity).

* **EU Regulations:** The European approach is built upon the principle that the right to privacy as one of the basic human rights as mentioned in the European Union declaration of human rights. The European commission has published the Opinion 8/2014 report on “the protection of individuals with regard to the processing of personal data” [83], in which some privacy challenges have been highlighted and guidelines and recommendation for user privacy protection have also been introduced. In addition, Privacy by Design principles [68] has been deeply studied from policy to engineering standpoint by the European Union Agency for Network and Information Security (ENISA) to enable developers and engineers with useful guidelines for private and data protection by design [86].
* **US Regulations**: As well-summarized in [82], the US regulation is a long legislative process based on Constitution amendments interpretation From US perspectives, many works have been carried out for user data usage regulation, from early 1970 with the “Fair Information Practice Principals” (FIPPs) to the Federal Trade Commission (FTC) report about privacy and security in a connected world [24], in which participants debated how FPPs should be applied to the IoT environment. It is worth noticing that EU philosophy focuses on the principle of privacy as a human right, whereas US philosophy takes also into account economic aspects, in the sense that too much privacy protectionism can hinder innovation in the field of personalized applications and services. But, it has been also shown in [87] that people trusting a firm are less concerned about their privacy and less reluctant to provide personal information.

Table ‎7‑1 Comparison between US-EU privacy principles

|  |  |
| --- | --- |
| United States | Europe |
| Privacy is not expressly mentioned is the Constitution | Privacy right is guaranteed in the European Declaration of Human Rights and the European Union (UE) Charter of fundamental freedoms |
| The individual relinquishes control of personal information voluntarily given to third parties | The individual retains ownership of personal information |
| Individual privacy is protected from the government | Individual privacy is protected by government from the private sector |

### The European Regulation: General Data Protection Regulation (GDPR)

#### The main principles of GDPR

Personal data represents all the information which can be used to identify a person. The most of this information is online identifiers, for example, the IP address, location data, and cookies. The protection of personal data is a link between the data set and the spread of information, the political and legal problems which surround them, and the way in which users see privacy [31].

GDPR defines personal data as: “*Any information relating to an identified or identifiable natural person (“data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”* (<https://gdpr-info.eu/>).

The biggest challenge in data protection is maintaining secure people’s privacy as well as their personal information while using the data.

Since 1995, the world has moved on and the Data Protection Directive (DPD)’s great principles which had, one time, protected our privacy is now obsolete. In 2018, the General Data Protection Regulation [37], more commonly known as the GDPR come into effect. The objectives of the law are to give European citizens better control and visibility of their private data. Members of UE will be able to know what kind of data is collected, for what goal and how long they are stored. All the economic actors which process European citizen data are concerning by the GDPR, consequently, it will impact area far beyond the reach of the UE. The principal issue for the company is to be able to know where our personal data and how to provide them to the citizen on a simple asking.

The GDPR is based on transparency and accountability, but the core of GDPR is data protection. The main principles of the GDPR are fairness and lawfulness, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality [32].

The following principles, such as lawfulness, fairness, and transparency describe data controllers’ obligations to have legitimate grounds for the processing of personal data. For ensuring the legality of the processing, transparency plays a vital role. Data subjects should be aware of the processing purposes and should be provided with suitable notification and information regarding its scope [33].

The purpose limitation refers to the obligation of data controllers to only use the collected data for specific and well-defined purposes. The usage of received information for other purposes has to be compatible with the initial one. Consent of the evidence subject laws can offer grounds to legitimize additional processing not related to the initial use. This principle can pose difficulties for the IoT. Very often vast amounts of data are collected for vague or broadly defined purposes.

Sensor fusion, or the linkage of existing but previously unconnected datasets, can offer new opportunities for data analytics that envisioned when the data collected. Invasive and unpredictable inferential profiling enabled by identification services that link devices and the data they collect [33].

Data controllers are needed mainly to use data that are relevant, adequate and limited to necessary to the primary purpose for which they processed. Data controllers must ensure that the collected data required in their intended processing scope, and that unnecessary data not collected beyond this scope. For the IoT, data controllers must establish that the data is obtained necessary to deliver their product or services [33].

What’s new in GDPR is that it has introduced a mandatory data breach notification regime.

Transparency needed in data processing which means that there has to be effective in communication with individuals. GDPR can cover this need because it is user-centric. All the information and the details provided to users in an accessible language that can be easily understood.

A company must know, at any time, what kind of data they are collecting, for what purpose, where are this data, how are they managed.

If a company cannot provide this information, it will receive a penalty of 20M euros or four percent of a company’s global annual revenue, whichever is higher.

In order to assure a better data protection, the GDPR add 5 new principles and concept:

* Accountability: Companies must be able to show that they follow the GDPR rules;
* Privacy by design: Data protection must be considerate as a part of a product’s conception process;
* DPO: The Data Protection Officer assure that his company follows the rules and his advices can ask if needed. He is the link between the company and the controllers;
* Security by default: Enhance the role of the security in a product value. The company must be able to detect a security breach and report it in less than 72 hours;
* Impact assessment: Companies have to realize impact assessment and provide a plan against a security breach.

Moreover, the GDPR included 2 new rights:

* Right To Restriction Of Processing: Requires companies to suspend further use while allowing existing data to continue to be stored;
* Right To Data Portability: Allows individuals to obtain all records of personal data held by the company.

#### GDRP rights and duties

In the scope of the GDPR any information needs to be taken literally. It can be a cookie, a name, an email address, a biometric element (facial recognition, fingerprint), a person's location, occupation, gender, a physical factor, health related data element, IoT identifiers, indeed anything.

The GDPR applies to controllers and processors. Data controller states how and why personal data is processed, while a processor is the party doing the actual processing of the data. Therefore, the controller could be any organization. A processor could be an IT firm doing the actual data processing. If controllers and processors are based outside the EU, the GDPR will still apply to them as long as they are dealing with data belonging to EU residents.

Both controllers and processors must make clear how they collect people's information, in what purposes they are using it and how they process the data.

Moreover, people have the right to access any information a company holds about them, and the right to know why that data is being processed, how long it is stored for, and who gets to see it.

##### The right to be forgotten

If the data is not relevant anymore, people can have their data deleted at any time. GDPR makes it clear that people can have their data deleted at any time if it is not relevant anymore. The controller is responsible for telling other organizations to delete any links of the data.

##### Data processing transparency

Organizations usually collect many different types of information about people, and even if one piece of data does not individuate someone, it could become relevant when combined with other data and determine someone's identity. This data will be reused and distributed to others in exchange for money and this is why the incoming GDPR guidelines are being introduced to give EU citizens more transparency about how their data is being used.

The main goal of GDPR is to ensure that personal data can only be collected legally, under strict conditions for a legitimate purpose.

##### Anonymization and pseudonymization under the GDPR

Recital 26 of the GDPR says that the principles of data protection should not apply to anonymous information, namely information that does not relate to an identified or identifiable natural person.

Quoting from Recital 26: Personal data which have undergone pseudonymization, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person.

In other words: pseudonymous data are protected by the GDPR whereas anonymous data are not.

#### Identified stakeholders in GDPR

GDPR regulation identifies the following 3 stakeholders in the value chain of personal data collection and processing:

* **Natural person**: corresponds to data owner in the sense that he/she is the source of personal data. The GDPR specifies the rights that a natural person has over his/her personal data.
* **Responsible of data processing**: it is any organism or a company which collects the personal data and process it to provide services. The GDPR specifies both the rights and the duties the responsible of data has over the data collected about a natural person.
* **Public authority**: it is the local authority in each country of the European Union that ensures the implementation of the GDPR and its corresponding local regulations. Furthermore, it is responsible to deal with the complaints lodged by natural person against any company about his/her personal data storing and processing. The GDPR specifies both the rights and the duties the public authorities have over the data collected about a natural person.

We summarize in what follows the main rights and duties lie with each stakeholder regarding the GDPR requirements.

#### Rights and duties of each stakeholder

##### Natural Person

The rights specified in the GDPR for alive natural person is summarized as follows:

* To have the full control over his/her own personal data
* Clear expression of consent on the processing of personal data (by email, checkbox, etc.)
* Give consent even for scientific research, and give separate consent for each processing of personal data
* Have a statement of consent expressed in clear and precise terms and not in unfair terms
* Know the identity of the data processor and controller
* Know the purposes of the treatments
* Be able to refuse or withdraw consent without suffering any prejudice
* The fundamental interests and rights of the data owner (natural person) override the controller's (data processor) interest
* Existence of a legitimate interest is subject to careful evaluation
* The rules governing the transfer of personal data from a group of companies to a company located in another country hold
* A legitimate interest of the controller or further processing of personal data should be prohibited where it is inconsistent with an obligation of legal, professional or other binding confidentiality
* The processing of particular data must be subject to harmonized conditions
* Any processing of personal health data for reasons of public interest should not result in personal data being processed for other purposes by third parties such as employers, insurance companies or banks
* Obtain access to one's personal data, rectification or erasure free of charge, and exercise of a right of objection
* Have all the necessary information that guarantees a fair and transparent treatment of personal data
* Be informed if personal data is obliged to provide, and the consequences if this data is not provided.
* Be informed when personal data is communicated to another recipient the first time
* Have an easy access to personal data collected at reasonable intervals to learn about the processing the data was subjected to and to verify its lawfulness
* Know the duration of the processing of its data and the logic that underlies their possible automated processing
* Have a "right to be forgotten"
* When personal data is provided on the basis of consent or for the implementation of a contract, the data owner has the right to receive his or her personal data in the case where the data is submitted to automated processing, in a structured, commonly used, machine-readable and interoperable format, and to forward them to another controller.
* Where technically possible, the data owner should have the right to have his data transferred directly from one data processor to another.
* Possibility to oppose any processing of any personal data in relation to their particular situation even if the processing is considered lawful with regard to the regulation
* Right to object at any time and free of charge to any processing related to prospecting purposes
* Not to be subjected to any decision taken solely on the basis of automated processing, which may include a measure involving the evaluation of certain personal aspects, which produces legal effects concerning the owner or affects him/her in a significant manner such as rejection of an online credit application, online recruitment practice, etc.
* The person concerned must be informed about this type of automatic processing; he/she must have the right to obtain a human intervention, to express his/her point of view, to obtain an explanation of the decision taken and to contest it.
* Automated decision-making and profiling based on particular categories of personal data should only be allowed under specific conditions.

##### Responsible of data processing

The rights of the responsible of data processing over user data are summed up in the following list:

* A processing considered as lawful if it is mandatory in the context of a contract or for the achievement of a contract
* A processing is lawful if is required to protect an essential interest that preserves the life of the person concerned or that of another natural person
* Preventing fraud is a legitimate interest for the processing of personal data
* Processing of personal data for purposes of prospecting can be considered to be realizing to meet an interest
* Transmitting personal data of clients and employees for internal administration purposes within a corporate group affiliated with a central body may be considered as a legitimate interest
* Processing of personal data (to the extent strictly necessary) for the purpose of guaranteeing the security of the network and information is of legitimate interest
* Derogations from the prohibition on dealing with particular categories of personal data should be explicitly provided for
* Particular categories of personal data may be processed only for purposes related to health and in the interest of individuals and society as a whole
* Additional conditions or limitations introduced by Member States must not impede the free movement of personal data within the Union where these conditions apply to the cross-border processing of such data
* In the case of anonymized data, the data controller is not obliged to request additional information from the data owner in order to comply with a provision of this Regulation.
* All information and communication for children when the processing concerns them should be written in clear and simple terms that the child can easily understand
* Reply within one month at the latest to any request from the person concerned
* Decision-making based on automatic processing of personal data, including profiling, should be permitted where authorized by Union law, or the law of a Member State to which a controller is subject, or the data owner has given explicit consent
* Ask the data owner to specify the data or the processes on which his request for information relates, in the case where the controller handles a large amount of data
* The retention of personal data should be lawful where it is necessary for the exercise of the right to freedom of expression and information, the fulfillment of a legal obligation, the performance of a public interest mission or exercise of the public authority that data controller is invested with.
* No obligation to provide an interoperable data format and communication to the data owner if the processing is necessary for the fulfillment of a legal obligation, for the implementation of a public interest mission, or for the exercise of the public authority
* No obligation to adopt or maintain technically compatible processing systems to ensure the right of the data owner to receive and transmit his/her data.

The duties of the responsible of data processing are summed up in the following list:

* Speudonomisation measures
* Save separately the identification data of the speudonomized data
* Indicate the persons authorized to perform data processing
* Prove that any person has consented to any processing on his personal data
* Ensure that consent is understood by the person
* Provide a clear, understandable, accessible statement of consent that does not contain unfair terms
* Accept any additional information provided by the data owner to facilitate the exercise of his/her rights

##### Public authorities

The rights of the public authorities over user data are summed up in the following list:

* Right to use all personal data in the context of a particular inquiry in the general interest.
* The legal basis for the processing of personal data should not apply to processing carried out by public authorities in the performance of their tasks
* Maintain and / or introduce additional conditions including limitations with respect to the processing of genetic, biometric, or health data
* Processing of personal data to meet objectives provided by constitutional law or public international law, associations of officially recognized religious character is carried out for reasons of public interest

The duties of public authorities over user data are summed up in the following list:

* Request for access to data must be in writing, reasoned, and occasionally;
* No access to an entire file,
* No process leading to data intersection
* Processing is subject to the same rules of protection of personal data
* In the context of a public interest mission or the exercise of public authority, any processing must have a basis in Union law or in the law of a Member State.
* the public entity must specify the controllers, the type of personal data being processed, the persons concerned, the purpose limitations, the retention period and other measures to ensure fair and lawful processing
* The European Data Protection Board established by this Regulation (hereinafter referred to as "the Committee") should be able to issue guidelines on "profiling".

# User Data Protection and Privacy Preservation: Best Practices

## Process

Maintaining security and privacy in industrial applications usually implies not only use of specific technologies, but also conforming to a set of international regulations. World Economic Forum published in [47] a protocol with the main safety and security requirements for IIoT products development and commercialization. For US, the National Institute of Standards and Technology (NIST) published a manufacturing profile providing details for implementing its Cybersecurity Framework in the plant [46]. It defines the functions required for the security framework and correlates these functions with process mission and objectives. A classification of risk based on these aspects is provided. It also published a draft revision of its SP 800-53 Security and Privacy Controls for Information Systems and Organizations, focused on how public and private sector organizations can maintain security and privacy in interconnected systems and devices such as their IoT and IIoT networks. This framework is a good start for implementing a security framework in an industrial application and it also approaches the privacy aspects related to transmitted data.

IT departments are required to find and apply suitable security mitigations schemes in order to handle the previously listed threats. Nevertheless, new threats and exploits emerge on a daily basis and products are deployed in different environments prone to different types of threats and risks. Thus, ensuring a proper level of security in an IoT system at any point of time is still a challenging task that need to be considered. To address this challenge, [65] advocates the following basic actions that need to be implemented while deploying of a new IoT system or when a significant system upgrades is performed:

1. First, perform a Business Impact Analysis (BIA) in order to assess the major consequences for the drop of one of the basic security attributes: confidentiality, integrity and availability in an IoT system. These consequences might include the impact from lost data, reduced sales, increased expenses, regulatory fines, customer dissatisfaction, etc. Performing a business impact analysis allows a business to determine the relevance of having a proper security design.
2. Second, achieve a Risk Assessment (RA) in order to assess security threats for the IoT system while considering their likelihood and impact. The result of this assessment would consider assigning a risk level for each security threat. The latter if classified as moderate or high must be mitigated, so that the deployed IoT system would be able to handle them.
3. Third, consider a Privacy Impact Assessment (PIA) in order to evaluate the Personally Identifiable Information (PII) that is collected, processed, or used in an IoT system. By doing so, the goal is to fulfill applicable legal requirements, determine risks and effects of manipulation and loss of PII.
4. Finally, implement specific measures for incident reporting and mitigation which would refer to the methodologies that allow becoming aware of any security issues that affect an IoT system. Furthermore, this includes steps towards the actual deployment of patches that mitigate the identified vulnerabilities.

## User Data Exploitation

There is a conflict between the end-users and the IoT, together with mobile application developers because the first group of people wants the data to be protected while the other wants to exploit the data in order to improve the applications. There are ways to make the services more intelligent without making the sensitive data of the users visible.

In the paper “Querying Invisible Objects: Supporting Data-Driven, Privacy-Preserving Distributed Applications” [42] there are presented some hypothetical situations in which the developers can handle sensitive data. For example, with a Mobile navigation application, real time traffic information is provided to the users, which can be very helpful. Unfortunately, right now the GPS location of each user is provided, and it can get very dangerous. In order to avoid the risk, a lot of traffic conditions can be calculated without using the actual location of each user. A new programmable mechanism named Object Expiration (OBEX) was implemented. This system can store sensitive data without providing access to their clients. The sensitive data is hidden in the system layer and so it is invisible to other users. In the usage scenario of OBEX there is a data producer who can collect and generate sensitive data and a data consumer who can use the data in order to make the services more intelligent and useful.

According to a report made by Open Web Application Security Project (OWASP), data vulnerability, insecure communications and unreliable authentication procedures are in the top 10 most security risks [42].

The privacy preservation means that not only the personal data of the user is preserved, but also the unlikability of different accesses to outsourced data. As showed before, personal data refers to the user’s identity and access patterns. The unlikability prevents the unauthorized parties to know that the same user is accessing the service and also to see if that one specific content is directly linked to one user. A necessary solution of the privacy prevention is the implementation of security services. Unfortunately, this is not sufficient because the provider can reveal to the client more information, besides the transmitted contents. In the article “Data Security and Privacy preservation in Cloud Storage Environments based on Cryptographic Mechanisms” [2] is presented a situation in which the client needs to communicate with another user without realizing that he can reveal data about his behavior, his likes, his acquaintances and so on. This example proves that the client’s privacy refers to more than just the encryption of the outsourced data.

When we think about the outsourced encryption data, we understand that some classical search algorithms can no longer be applied. Therefore, the searchable encryption needs to combine confidentiality with search functionality. The Cloud server needs to have the permission to search the encrypted data using a trapdoor information that the client provides. The client has the ability to decrypt the data file locally, and therefore the searchable encryption saves bandwidth consumption [43].

## User Data Back-up

User data protection is an important issue for most of data storage or data processing in all development applications. It exists the possibility of losing data due to the equipment failure, human error or other circumstance, even when the computer and storage hardware have become reliable over time [34].

Many strategies to back up the data, let's choose Network data protections for example. Network data protection it's a strategy that involves sending a copy of data over a proprietary or public network to an off-site server. The server could be hosted by a third-party service provider, who charges the backup customer a fee based on different criteria like capacity, bandwidth, number of users. Also, the recovery of data is a concern for many businesses because it's a critical operation to restore data as quickly as possible. Thus, data protection and restoration are part of risk mitigation for most any company or institution, so it's desirable to have improvements in data protection. User data can be measurement data provided by sensors or personal data. Measurement data can be temperature values, gas values, humidity values [34].

User data may be stored and shared on a hard drive, cloud-based storage, USB devices, paper, e-mails, mobile devices and on IT management systems. To comply with GDPR legislation, each of these devices needs to be securely protected by implementing the following data protection strategies:

* Restrict access to data on a ‘need to know’ basis;
* Give employees individual logins with individual access levels;
* Have a protocol which ensures that employees change the passwords regularly;
* Use encryption when sending and sharing data;
* Where possible, anonymize data when sending to third parties;
* Ensure all computers, memory sticks, hard drives and backups are password protected;
* Ensure all paperwork is locked away in files at the end of the day – this applies when working from home too;
* Operate a ‘clean desk policy’; that is, not leaving personal data lying around on the desk;
* Ensure all employees receive in-depth training on personal data;
* Ensure all archived data is encrypted;
* Securely dispose of any unused, unneeded data, or anonymize it;
* Regularly check that the network is secure when having multiple branches [35].

## Privacy by design

Privacy by Design (PbD) [55] aims at protecting privacy by including it into the design specification of a given service or software. It has been developed by Ontario's Information and Privacy Commissioner, Dr. Ann Cavoukian, in the 1990s, as a response to the growing threats to online privacy that were beginning to emerge at that time.

### The 7 Foundational Principles of PbD

Global and local businesses are starting to implement the 7 Foundational Principles of PbD, which are presented below [78]:

* Proactive not Reactive: The Privacy by Design (PbD) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen.
* Privacy as the Default: The personal data are automatically protected in any given system or product. There is no action required on the part of the individual to protect their privacy, it is built into the system by default.
* Privacy Embedded into Design: Privacy by Design is embedded into the design and architecture of systems or product. The privacy becomes essential in the core functionality being delivered.
* Full Functionality: Privacy is embedded in a way that the functionalities are not impaired. Privacy should not have to compete with other legitimate interests, design objectives or technical capabilities.
* End to End security: Throughout the life-cycle, strong security is essential to privacy. All data are securely retained, and then securely destroyed at the end of the process. Privacy by design ensures secure lifecycle management of information.
* Visibility and Transparency: Visibility and transparency are essential to establishing accountability and trust. The component parts and operations remain visible and transparent to both users and providers.
* Respect for User Privacy: Privacy by Design is designed around the interests and needs of individual users, who have the interest in the management of their own personal data. Users should have strong privacy defaults and appropriate notice and empowering user-friendly options.

### Privacy by design and GDPR

The article 25 of the General Data Protection Regulation (GDPR) says “*data protection by design and default*”, requires to “*implement appropriate technical and organizational measures*” throughout any data processing project. User privacy must be considered at the design stage of any project, during which you must process and store as little data as possible, for as short a time as possible.

Organizations need to be aware of the personal data that they are processing, and that this data is being processed in compliance with the law.

One of the key changes to be brought into the GDPR is that of “Privacy by Design” along with “Privacy by Default”. Companies are now obliged to consider data privacy during design stages of all projects along with the lifecycle of the relevant data processes.

The Information Commissioner's Office (ICO) encourages organizations to seriously consider privacy and data protection throughout a project lifecycle, including when:

* Building new IT systems to store or access personal data,
* Needing to comply to regulatory or contractual requirements,
* Developing internal policies with privacy implications.

# Conclusion

As the number of IoT devices continues to increase, more and more automation will be needed for both individual users and industrial environments. Therefore, as the automation levels rise within IoT systems, also the hardware and software vulnerabilities will increase.

In the close future, information from IoT devices is going to be handled by proxy network servers, because end devices used nowadays practically have few, if no security features. Therefore, more work should be spent on designing IoT devices.

Still, before better standards concerning privacy protection of individual data and better security rules on transmission procedures and cloud/ information storage, security of sensors and wearables will stay poor. The variety of the software and hardware in the IoT area gives solid market competition, but it also provides a security issue since there is no general “system”. The “system” is dynamically characterized by the request of the customer and the response from the vendors. The capacity to design secure IoT devices relies on the meaning of security standards and agreements between vendors. Providers will handle the access to devices in the cloud, but they cannot grant 100% security against unapproved access. Thus, it is fundamental to exist cooperation between vendors in order to develop a secured IoT world.

The state of the art about user privacy protection aims to take notice of the current situation regarding personal data protection in general and user privacy in particular, upon which it would be possible to design and implement a user-centric approach for user privacy protection based on principles of “Privacy by design” to encompass current regulations in the matter and well balance between the right to data privacy and the innovation possibilities in a propitious domain for open and shared data. Privacy protection enables users to take full control of their personal data:

1. to have the right to consent/deny sharing them,
2. to be informed about all the processes the data are subject to and the conclusions drawn from them (inferences, cross-analysis, etc.),
3. to be able to retract the consent for any reason, and
4. to modify/delete definitely the data.

Finally, we believe that a trustworthy relationship between application providers and the consumers may foster the adoption of many home/individual-centric applications that do improve the quality of life such as e-health, home automation, e-commerce, e-education, e-bank, e-sport, etc.

**Acronyms**

CP-ABE Ciphertext-Policy Attribute-Based Encryption

ENISA European Union Agency for Network and Information Security

FIPP Fair Information Practice Principals

FTC Federal Trade Commission

GDPR General Data Protection Regulation

ICO Information Commissioner’s Office

IM Instant Messaging

OpenPDS Open-source Personal Data Store

PbD Privacy by Design

TPM Trusted Platform Module

WSN Wireless Sensor Networks

**References**

[1] Ali, B., & Awad, A. I. (2018). Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes. Sensors, 18(3), 817.

[2] “Best WiFi and Bluetooth Smart Door Locks”: https://www.postscapes.com/wireless-door-locks/

[3] Echo Spot - White: <https://www.amazon.com/dp/B073SRJD46/ref=as_li_ss_tl?th=1&linkCode=sl1&tag=iotlist-20&linkId=0267e2f731455a061d520c05aee61ccf>

[4] August Smart Lock, 3rd Gen technology: <https://www.amazon.com/August-Smart-Lock-3rd-technology/dp/B0752XNC8M>

[5] Nest Learning Thermostat: <https://nest.com/thermostats/>

[6] Awair Glow: <https://getawair.com/products/awair-glow>

[7] Cujo: <https://www.amazon.com/gp/product/B017B53DLY/ref=as_li_qf_sp_asin_il_tl?ie=UTF8&tag=iotlist-20&camp=1789&creative=9325&linkCode=as2&creativeASIN=B017B53DLY&linkId=45791ee217e705460b4a8efbb1cace17>

[8] Keen Home: <https://www.amazon.com/gp/product/B00YCAWCV4/ref=as_li_qf_sp_asin_il_tl?ie=UTF8&camp=1789&creative=9325&creativeASIN=B00YCAWCV4&linkCode=as2&tag=iotlist-20&linkId=QAXBKT6JPYQ3EZKJ>

[9] Netatmo Welcome: <https://www.amazon.com/gp/product/B00X5X1XPU/ref=as_li_qf_sp_asin_il_tl?ie=UTF8&camp=1789&creative=9325&creativeASIN=B00X5X1XPU&linkCode=as2&tag=iotlist-20&linkId=HGF4GGVC3ZBYIXAU>

[10] IoT Devices-A Complete Guide: <https://internetofthingswiki.com/iot-devices/>

[11] IoT devices (internet of things devices): <https://internetofthingsagenda.techtarget.com/definition/IoT-device>

[12] Internet of Things - number of connected devices worldwide 2015-2025: <https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/>

[13] Sivaraman, V., Gharakheili, H. H., Vishwanath, A., Boreli, R., & Mehani, O. (2015, October). Network-level security and privacy control for smart-home IoT devices. In Wireless and Mobile Computing, Networking and Communications (WiMob), 2015 IEEE 11th International Conference on (pp. 163-167). IEEE.

[14] Linden Tibbets and Jesse Tane. (2012). IFTTT. [Online]. Available: <https://platform.ifttt.com/>

[15] Amazon. (2012). Alexa. [Online]. Available: <https://developer.amazon.com/alexa>

[16] Ali. (2015). Alibaba Smart Living. [Online]. Available: <https://www.aliplus.com/>

[17] Samsung. (2014). SmartThings. [Online]. Available: <https://www.smartthings.com/>

[18] Fernandes, E., Jung, J., & Prakash, A. (2016, May). Security analysis of emerging smart home applications. In 2016 IEEE Symposium on Security and Privacy (SP) (pp. 636-654). IEEE.

[19] M. Leo, F. Battisti, M. Carli, and A. Neri, “A federated architecture approach for Internet of Things security”, in Euro Med Telco Conference (EMTC), 1-5, 2014.

[20] P. N. Mahalle, B. Anggorojati, N. R. Prasad, and R. Prasad, “Identity authentication and capability based access control (iacac) for the internet of things”, J. of Cyber Security and Mobility, vol. 1, 309-348, 2013.

[21] Blowers, M., Iribarne, J., Colbert, E., & Kott, A. (2016). The Future Internet of Things and Security of its Control Systems. arXiv preprint arXiv:1610.01953.

[22] Embedded Hardware Security for IoT Applications (2016): <https://www.securetechalliance.org/wp-content/uploads/Embedded-HW-Security-for-IoT-WP-FINAL-December-2016.pdf>

[23] N. Parikshit Mahalle, “Identity Authentication and Capability Based Access Control (IACAC) for the Internet of Things”, Journal of Cyber Security and Mobility, Vol. 1, 309–348. 2013

[24] “Internet of Things: privacy and security in a connected world”, US Federal Trade Commission, Staff report, 2015. <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>

[25] T. Gupta, R.P. Singh, Mahajan, A. P. J. J. R. Bolt: Data management for connected homes. In Proceedings of the 11th USENIX Symposium on Networked Systems Design and Implementation (NSDI 14) (2014), pp. 243–256

[26] B. Zhang, N. Mor, J. Kolb, D.S. Chan, K. Lutz, E. Allman, J. Kubiatowicz, (2015, July). “The Cloud is Not Enough: Saving IoT from the Cloud”. In HotCloud

[27] K. Sonar, H. Upadhyay (2014). A survey: DDOS attack on Internet of Things. International Journal of Engineering Research and Development, 10(11), 58-63.

[28] Koydemir, H. C., & Ozcan, A. (2018). Wearable and Implantable Sensors for Biomedical Applications. Annual Review of Analytical Chemistry, (0).

[29] Sun, W., Cai, Z., Li, Y., Liu, F., Fang, S., & Wang, G. (2018). Security and privacy in the medical Internet of Things: A review. Security and Communication Networks.

[30] Ali, B., & Awad, A. I. (2018). Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes. Sensors, 18(3), 817.

[31] Pavlou, P. A. (2011). State of the information privacy literature: Where are we now and where should we go?. MIS quarterly, 977-988.

[32] Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. International Journal of Market Research, 59(6), 703-705

[33] Wachter, S. (2018). GDPR and the Internet of Things: Guidelines to Protect Users’ Identity and Privacy.

[34] Banasik, A., Gasiorowski, T. M., Jose, D. M. L., & McGrath, G. D. (2018). U.S. Patent Application No. 15/844,940.

[35] Beacham, J. (2018). Is your practice GDPR ready?. In Practice, 40(3), 124-125.

[36] Domingo-Ferrer, J. (2016). Directions in Big Data Anonymisation, Universitat Rovira i Virgili, Tarragona, Catalonia.

[37] PPAI White Paper (2018). The General Data Protection Regulation.

[38] Doc Searls (2012). The intention economy: When Customers Take Charge,

[39] MesInfos websites : http://mesinfos.fing.org

[40] Solid ant Inrupt websites; https://solid.mit.edu/; https://www.inrupt.com/

[41] Midata Innovationlan website: http://www.midatalab.org.uk/

[42] Liu, Y., Song, Z., & Tilevich, E. (2017, September). Querying Invisible Objects: Supporting Data-Driven, Privacy-Preserving Distributed Applications. In Proceedings of the 14th International Conference on Managed Languages and Runtimes (pp. 60-72). ACM.

[43] Kaaniche, N., & Laurent, M. (2017). Data security and privacy preservation in cloud storage environments based on cryptographic mechanisms. Computer Communications, 111, 120-141.

[44] Ann R. Thryft, “What's Needed to Secure the Industrial IoT”, EETimes online magazine, Apr. 2018.

[45] Trend Micro Incorporated, “SCADA in the Cloud. A Security Conundrum?”

[46] National Institute of Standards and Technology (NIST), US Department of Commerce, “Cybersecurity Framework Manufacturing Profile”, Sept. 2017.

[47] World Economic Forum, Center for the Fourth Industrial Revolution Protocol Design Networks, “Industrial Internet of Things Safety and Security Protocol”, Apr. 2018.

[48] ReliteQ, Real Time Remote Control and Monitoring, website: <http://www.realiteq.com/>

[49] Skkynet, website: <https://skkynet.com/>

[50] IoT ONE, Accelerating the Industrial Internet of Things, website: <https://www.iotone.com/>

[51] L. H. Newman, “The Sensors That Power Smart Cities Are A Hacker's Dream”,

[52] Iconlabs, Floodgate Security Framework

[53] Kiaora IoT device security, eclipse project proposal, available online at: <https://dev.eclipse.org/mhonarc/lists/iot-wg/msg00476.html>

[54] German Federal Office for Information Security BSI, Protection Profile Common Criteria PP Configuration Machine Readable Electronic Documents: <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Reporte/ReportePP/pp0090b_pdf.html>

[55] Internet Engineering Task Force (IETF) / rfc7696 - Guidelines for Cryptographic Algorithm Agility and Selecting Mandatory-to-Implement Algorithms: <https://trac.tools.ietf.org/html/rfc7696>

[56] National Institute of Standards and Technology (NIST), US Department of Commerce, “Post-Quantum Cryptography”: <https://csrc.nist.gov/projects/post-quantum-cryptography>

[57] Rescorla, E., "HTTP Over TLS", RFC 2818, DOI 10.17487/RFC2818, May 2000.

[58] Shelby, Z., Hartke, K. and C. Bormann, "The Constrained Application Protocol (CoAP)", RFC 7252, DOI 10.17487/RFC7252, June 2014.

[59] Kushalnagar, N., Montenegro, G. and C. Schumacher, "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals", RFC 4919, DOI 10.17487/RFC4919, August 2007.

[60] Moustafa, H., Tschofenig, H. and S. De Cnodder, "Security Threats and Security Requirements for the Access Node Control Protocol (ANCP)", RFC 5713, DOI 10.17487/RFC5713, January 2010.

[61] Atkins, D. and R. Austein, "Threat Analysis of the Domain Name System (DNS)", RFC 3833, DOI 10.17487/RFC3833, August 2004.

[62] Nikander, P., Kempf, J. and E. Nordmark, "IPv6 Neighbor Discovery (ND) Trust Models and Threats", RFC 3756, DOI 10.17487/RFC3756, May 2004.

[63] Parthasarathy, M., "Protocol for Carrying Authentication and Network Access (PANA) Threat Analysis and Security Requirements", RFC 4016, DOI 10.17487/RFC4016, March 2005.

[64] Bormann, C., Ersue, M. and A. Keranen, "Terminology for Constrained-Node Networks", RFC 7228, DOI 10.17487/RFC7228, May 2014.

[65] O. Garcia-Morchon, S. Kumar, M. Sethi, State-of-the-Art and Challenges for the Internet of Things Security, draft-irtf-t2trg-iot-seccons-14, <https://tools.ietf.org/id/draft-irtf-t2trg-iot-seccons-14.html>

[66] Baldini, G., Peirce, T., Handte, M., Rotondi, D., Gusmeroli, S., Piccione, S., Copigneaux, B., Gall, F. L., Melakessou, F., Smadja, P., Serbanati, A., and Stefa, J. (2013). Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems, chapter 4: Internet of Things Privacy, Security and Governance, pages 207–224. River Publishers.

[67] Bohli, J.-M., Langendörfer, P., and Skarmeta, A. F. G. (2013). Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems, chapter 5: Security and Privacy Challenge in Data Aggregation for the IoT in Smart Cities, pages 225–244. River Publishers.

[68] Cavoukian, A. et al. (2009). Privacy by design: The 7 foundational principles. implementation and mapping of fair information practices. Technical report, Information and Privacy Commissioner of Ontario.

[69] de Montjoye, Y.-A., Wang, S. S., Pentland, A., Anh, D. T. T., Datta, A., et al. (2012). On the trusted use of large-scale personal data. IEEE Data Eng. Bull., 35(4):5–8.

[70] Sicari, S., Rizzardi, A., Grieco, L., and Coen-Porisini, A. (2015). Security, privacy and trust in internet of things: The road ahead. Computer Networks, 76:146 – 164.

[71] Smith, H. J., Dinev, T., and Xu, H. (2011). Information privacy research: an interdisciplinary review. MIS quarterly, 35(4):989–1016.

[72] Serrano-Alvarado, P. and Desmontils, E. (2013). Personal linked data: a solution to manage user’s privacy on the web. In Atelier sur la Protection de la Vie Privée (APVP).

[73] Oliveira, L. B., Aranha, D. F., Gouvêa, C. P., Scott, M., Câmara, D. F., López, J., and Dahab, R. (2011). Tinypbc: Pairings for authenticated identity-based non-interactive key distribution in sensor networks. Computer Communications, 34(3):485–493.

[74] Vincent, J., Porquet, C., Borsali, M., and Leboulanger, H. (2011). Privacy protection for smartphones: an ontology-based firewall. In Information Security Theory and Practice. Security and Privacy of Mobile Devices in Wireless Communication, pages 371–380. Springer.

[75] Machanavajjhala, A., Kifer, D., Gehrke, J., and Venkitasubramaniam, M. (2007). L-diversity: Privacy beyond k-anonymity. ACM Transactions on Knowledge Discovery from Data (TKDD), 1(1).

[76] Sweeney, L. (2000). Uniqueness of simple demographics in the US population. Technical report, Technical report, Carnegie Mellon University.

[77] Sweeney, L. (2002). k-anonymity: A model for protecting privacy. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 10(05):557–570.

[78] Samarati, P. (2001). Protecting respondents’ identities in microdata release. Knowledge and Data Engineering, IEEE Transactions on, 13(6):1010–1027.

[79] Li, N., Qardaji, W. H., and Su, D. (2011). Provably private data anonymization: Or, k-anonymity meets differential privacy. CoRR, abs/1101.2604, 49:55.

[80] Zhang, K., Yang, K., Liang, X., Su, Z., Shen, X., and Luo, H. (2015). Security and privacy for mobile healthcare networks: from a quality of protection perspective. Wireless Communications, IEEE, 22(4):104–112.

[81] Liu, X., Zhang, Q., and Li, Z. (2015). Secure data aggregation with privacy-protection in smart grid. In Computer Science and Applications: Proceedings of the 2014 Asia-Pacific Conference on Computer Science and Applications (CSAC 2014), Shanghai, China, 27-28 December 2014, page 63. CRC Press.

[82] McNealy, J. and Flowers, A. (2015). Privacy in a Digital, Networked World: Technologies, Implications and Solutions, chapter Privacy Law and Regulation: Technologies, Implications, and Solutions, pages 189–205. Springer International Publishing, Cham.

[83] WP229 (2014). Opinion 8/2014 on the on recent developments on the internet of things. Technical report, The working party on the protection of individuals with regard to the processing of personal data. European commission.

[84] Malekzadeh, M., Clegg, R. G., Cavallaro, A., and Haddadi, H. (2018). Protecting sensory data against sensitive inferences. In Proceedings of the 1st Workshop on Privacy by Design in Distributed Systems, W-P2DS’18, pages 2:1–2:6, New York, NY, USA. ACM.

[85] Osia, S. A., Shamsabadi, A. S., Taheri, A., Katevas, K., Rabiee, H. R., Lane, N. D., and Haddadi, H. (2017). Privacy-preserving deep inference for rich user data on the cloud. arXiv preprint arXiv:1710.01727.

[86] Le Métayer, D., Danezis, G., Hansen, M., Hoepman, J.-H., Tirtea, R., Schiffner, S., and Domingo-Ferrer, J. (2014). Privacy and Data Protection by Design - from policy to engineering. ENISA Report.

[87] Schoenbachler, D. D. and Gordon, G. L. (2002). Trust and customer willingness to provide information in database-driven relationship marketing. Journal of interactive marketing, 16(3):2–16.

[88] Kinney, S. L. (2006). Trusted Platform Module Basics: Using TPM in Embedded Systems (Embedded Technology). Newnes publisher.

[89] Perrig, A., Szewczyk, R., Tygar, J., Wen, V., and Culler, D. (2002). Spins: Security protocols for sensor networks. Wireless Networks, 8(5):521–534.

[90] Thilakanathan, D., Calvo, R., Chen, S., and Nepal, S. (2013). Secure and controlled sharing of data in distributed computing. In Computational Science and Engineering (CSE), 2013 IEEE 16th International Conference on, pages 825–832. IEEE.

1. The internet of things: Are organizations ready for a multi-trillion dollar prize? Technical report, Capgemini Consulting. 2014. [↑](#footnote-ref-1)