Computer Networks 112 (2017) 237–262

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

Review article

Access control in the Internet of Things: Big challenges and new opportunities

Aafaf Ouaddah[a,*], Hajar Mousannif[b], Anas Abou Elkalam[a], Abdellah Ait Ouahman[a]

[a] OSCARS Laboratory, Ensa of Marrakesh, Cadi Ayyad University, Marrakesh, Morocco
[b] LISI Laboratory, FSSM, Cadi Ayyad University, Marrakesh, Morocco

ARTICLE INFO

Article history:
Received 7 June 2016
Revised 5 November 2016
Accepted 8 November 2016
Available online 9 November 2016

MSC:
00-01
99-00

Keywords:
Internet of Things
Security
Privacy
Access control

ABSTRACT

In this paper, an extensive state of the art review of different access control solutions in IoT within the Objectives, Models, Architecture and Mechanisms (OM-AM) way is provided. An analysis of the security and privacy requirements for the most dominant IoT application domains, including Personal and home, Government and utilities, and Enterprise and industry, is conducted. The pros and cons of traditional, as well as recent access control models and protocols from an IoT perspective are highlighted. Furthermore, a qualitative and a quantitative evaluation of the most relevant IoT related-projects that represent the majority of research and commercial solutions proposed in the field of access control conducted over the recent years (2011- 2016) is achieved. Finally, potential challenges and future research directions are defined.

1. Introduction

Have you ever imagined your clothes, furniture, cars, household lights or even your coffee pots have their own Twitter accounts, interact with social networks and send data to the cloud, enabling aggregation of data from different devices and aspects of your lives? That is the era of The Internet of Things where the barriers between the real and cyber worlds are increasingly annihilated by turning out every day physical devices to smart objects. This is a huge and fundamental shift. When we start making things intelligent, it is going to be a great engine for creating new products and new services to improve peoples everyday lifestyle, spawn new businesses and make hospitals, factories, roads, airways, offices, retail stores and public buildings, smarter. So what will really happen when things that heretofore were blind and mute; talk, wash, hear and even think? These billions of devices are, actually, pervading our surrounding environment and even our bodies. For the sake of improving our lifestyle, they are tracking us and increasingly encroaching on our private and intimate spaces. Indeed, smart meters deduce when we shower, cars know when we do not go to work, wearable medical devices know our weight, and mobiles know how we feel [1]. As consequence, the success or failure of this revolutionary evolution will be determined by two key challenges: security and privacy. Since lack of trust about privacy will result in decreased adoption among users. Actually, a study [2] about the future of digital trust released by orange has shown that 78% of consumers think that it is hard to trust companies when it comes to use their personal data. The EU Commissions public consultation on IoT governance and the FTCs latest debates have shown in a clear way that there is an urgent need for implementing security measures for minimizing the impact of a cyber-attack and unlawful profiling and surveillance of individuals.

More specifically, in this paper, we explore access control area as one of the most crucial aspect of security and privacy in IoT. Actually, a robust security study should identify who has access to what, when and in which conditions. The Common Criteria defines an organizational security policy as: a set of security rules, procedures, or guidelines imposed (or presumed to be imposed) now and/or in the future by an actual or hypothetical organization in the operational environment [3]. Such an organizational security policy usually relies on an access control policy [4]. An access control model is often used to rigorously specify and reason on the access control policy (e.g., to verify its consistency). However, the model does not specify how the security policy is enforced. The enforcement should be realized by technical security mechanisms, such as credentials, Cryptographic transformations (e.g., signature, encryption), access control lists (ACL), and firewalls among others.

* Corresponding author.
E-mail address: aafafouaddah@gmail.com (A. Ouaddah).

http://dx.doi.org/10.1016/j.comnet.2016.11.007
1389-1286/

Providing an adequate access control model for IoT services is a vital but challenging topic. Indeed, authentication and authorization issues have been intensively investigated through existing protocols for use cases outside constrained environments. However in constrained environments, those issues are still in their infancy. In fact, additional and different requirements pose challenges for the use of various security protocols. In particular, the need arises for a dynamic and fine-grained access control mechanism, where users/resources are constrained.

Our paper is the first, to the best of our knowledge, which surveys and focuses, in an extensive way, on access control in IoT environments, and presents in a comprehensive way models, protocols, and framework solutions in IoT. In fact, there are other surveys that have tried to address issues related to the IoT paradigm:

Maw et al. [5] deals with access control issues but only in Wireless Sensors Network (WSN) environments.

Sicari et al. [6] analyzes security, privacy and trust in IoT context but does not handle the access control issue in an exclusive way.

Atzori et al. [7] analyzes IoT enabling technologies and existing middleware solutions, and presents security and privacy open issues but it does not establish the link between the models and the mechanisms.

Miorandi et al. [8] picks out the main challenges in IoT, dealing with data confidentiality, privacy, and trust with respect to security requirements and examines the main research contexts (i.e., impact areas, projects, and standardization activities).

Weber [9] describes the security and privacy challenges but only from a legislative perspective.

Yan et al. [10] focuses only on trust management in IoT.

Roman et al. [11] explores the pros and cons of centralized and distributed architectures of security and privacy in IoT, with an analysis of the principal attack models and threats.

Gubbi et al. [12] provides a general overview of various IoT aspects, such as involved technologies, applications, cloud platforms, architecture, energy consumption and security issues, quality of service and data mining implications.

However, none of the works presented above surveys in a comprehensive way access control issue in the Internet of Things. This paper extends and improves our prior work in [13,14] with significant new materials. More specifically, our contributions can be summarized as follows:

- Definition of a reference model for comprehensively analyzing and reviewing authorization process in IoT based on the OM-AM way .
- Analysis of the main characteristics and security requirements that make IoT and its main domains application a unique ecosystem compared to previous Information Technology (IT) infrastructures. With respect to those properties, a number of security and privacy preserving objectives are identified.
- Review of the literature about access control solutions in IoT within the defined OM-AM reference model.
- Highlight for each refereed access control solution its own strengths and weaknesses.
- Elaboration of a qualitative and a quantitative evaluation: based on the fourteen identified Security and Privacy-Preserving objectives.
- Guide for the reader to know the pros and cons and the usability of current and traditional access control models and protocols from an IoT perspective.
- Extraction of the mains challenges, potential future research directions and opportunities of access control in IoT

The remainder of this paper is organized as follow: Section 2 defines the four layer of our adopted OM-AM reference model that we follow to analyze and review the authorization process in IoT. Section 3 discusses and reviews the literature for each layer separately. Section 4 evaluates in a qualitative and quantitative way the studied solutions. Section 5 extracts the main challenges of access control in IoT. Section 6 gives hints of potential and future research directions. Section 7 concludes our paper.

2. A proposed (OM-AM) authorization reference model for IoT

Access control: definition and background: Authentication and access control technologies are known as the main elements to address the security and privacy issues in the Internet of Things. Actually, any effective access control system should satisfy the main security properties of confidentiality (preventing unauthorized divulgation of resources), integrity (preventing resource to be modified without authorization resources), and availability (assuring access to resource by legitimate users when needed). More details about access control models, policies and mechanism could be found in [15]. A complete access control system covers the following three functions [16]: Authentication [17], Authorization [18] and Accountability. In this survey, we focus only on Authorization. Authentication and accountability are out of the scope of this paper.

2.1. OM-AM authorization reference model

2.1.1. Motivation

Authorization involves the following phases: defining a security policy (set of rules), selecting an access control model to encapsulate the defined policy, implementing the model and enforcing the access rules. Each phase requires specific tools to be deployed. We cite as example: Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) method [19] that can be used as a basis to derive the security policy, the RBAC model [20] to define an access control model, Extensible Access Control Markup Language (XACML) standard [21] to propose an architecture and language to implement security policy rules, and Oauth2.0 framework [22] which includes the authentication phase but proposes also an architecture (including entities and workflow) to implement the authorization function. Unfortunately, we notice a big confusion between those tools in the literature and even in the terms used in authorization field. As a result, we find an illegitimate comparison between some of the above tools and their fitness to IoT environment. That is due to the lack of a normalization of the terms used in authorization process in the literature. To fill this gap and avoid any confusion, we find that it is a worthwhile idea to propose a reference model as normalization to authorization process. By analogy to OSI (Open Systems Interconnection) 7 layers network protocol stack, we opt for the four layer OM-AM framework coined in [23], or more informally the OM-AM way, to analyze the authorization process. OM-AM stands for Objective, Model, Architecture, and Mechanism. The objective and model (OM) layers articulate what the security objectives are and what should be achieved, while the architecture and mechanism (AM) layers address how to meet those requirements. Like OSI 7 layers, each OM-AM framework layers mapping to adjacent layers is many-to-many. In other words, security policy can be formalized with many access control models as they can support different security policies. Moreover an access control model can be supported by multiple architectures, while a specific architecture can support multiple models, and do not necessarily comply with the top-down waterfall-style software engineering process.

Table 1
OM-AM Framework for authorization process.

Objective	security policy, risk assessment octave, EBIOS methods, ISO/EIC 27002/27005 standards etc)
Model	Authorization model (e.g. RBAC, ABAC, UCON)
Architecture	Frameworks, protocols (XACML, OAuth, UMA)
Mechanisms	Hardware and software tools: (ACLs, Routers, Encryption, Audit logs, IDS, Antivirus software, Firewalls, Smart cards, Dial-up call-back systems, Alarms and alerts etc)

2.1.2. Concept and terminology: the OM-AMs four layers defined and functions explained

The OM-AM model has four layers that are stacked this way starting from the high-level specification till low-level enforcement mechanisms and implementation as explained below and depicted in Table 1.

- Objectives: this layer serves as a referential background that all security and access control actions and measurements are based on. The main function of this layer consists in defining an access control policy that defines the (high-level) rules according to which access control must be regulated. This layer contains a variety of commonly needed functions: expression of needs by conducting a circumstantial study of the system to be secured and its environment, drawing the perimeter and the scope to be targeted, conducting a Risk Assessment and identification of Security objectives etc. A whole arsenal of methodologies, methods and tools are used in this layer like: Risk Assessment Methods, ISO/IEC 27002 and 27005. OTACE EBIOS, MAHARI, CRAMM, OWASP among others.
- Authorization model: after defining the security requirement, objectives and scopes to be secured in the system, one of the major difficulties lies in the interpretation of, often complex and sometimes ambiguous, real world security policies and in their translation in well-defined and unambiguous rules enforceable by a computer system. Here, where the role of Authorization model layer comes to bridge the gap between high-level policies and low-level mechanisms by defining means of how authorization rules should be applied to protect resources. Actually, an Authorization model is a formalism (often mathematical) for representing in a clear and unambiguous way the security policy. It helps to abstract it (i.e. reduce its complexity) and to facilitate its understanding. It can be used to verify that the policy is complete and consistent. Popular authorization models include Discretionary model DAC, Mandatory model MAC, RBAC and its extensions, Attribute-Based Access Control (ABAC) model [24], OrBAC model [25] and Usage Control (UCON) presented by [26–28] among many others. Such models are defined mostly in terms of subjects and objects and possible interactions between them but there are also other models that are based on different parameter like: trust, privacy, knowledge, and context. A model can also be hybrid and include more than one model in order to tackle the more heterogeneous needs of an organization. Only after the access control model is chosen can the right technology and both authentication and access control mechanisms be selected and implemented.
- Architecture: this layer describes the entities, the workflow and interactions between them (centralized or decentralized). Given this set of entities, several authorization sequences can be defined for example: Push, Pull or Agent sequence [29]. The most popular authorization architecture is published by an ISO standard for the access control framework ISO/IEC 10181-3 [30] that defines the main features of the reference monitor. According to that standard, a reference monitor consists of two basic components: an access enforcement facility (AEF) or a policy enforcement point (PEP) and an access decision facility (ADF) or a policy decision point (PDP). Every request made by a subject is intercepted by the AEF/PEP and then forwarded to the ADF/PDP for an access decision evaluation. The ADF/PDP may reply either yes/grant or no/deny depending on the security policy, while the AEF/PEP enforces this decision appropriately. Tools in this layer could be in form of protocols or framework such as Oauth protocol and XACML standard.
- Mechanisms: it defines the low level (hardware and software) functions to enforce policies and define how access requests are evaluated against those policies. Actually, configuring access control policies is a non-trivial and highly critical process, and it should be subject to periodic review and verification to ensure that security policies are correctly expressed and implemented [31]. Proposed verification methods include formally testable policy specification [32], detection of anomalies or connecting rules via segmentation technique [33], and analysis tools that enable policy administrators to evaluate policy interpretations [34]. A plethora of tools belongs to this layer such as: ACLs, Routers, Encryption, Audit logs, IDS, Antivirus software, Firewalls, Smart cards, Dial-up call-back systems, alarms and alerts among others.

In this way, the OM-AM framework allows us to:

- Define in a perspicuous way the boundaries as well as the relationship between each phase in the authorization process, since each phase matches a specific layer.
- Discuss each phase independently from the other. As an example, discuss the security requirements separately from the mechanism required for its implementation.
- Compare in a vertical way different access control policies that encapsulate the same security policy or different architectures that implement the same access control model and different mechanisms that enforce the access control architecture.
- Compare in a horizontal way within one layer for example between different access control models/mechanisms.
- Design each layer separately: for example, design mechanisms that are able to enforce multiple policies [35]. This latter aspect is particularly crucial since it will give great flexibility and scalability to the whole access control system. In fact, if a tool in one layer is tied to a specific component in another layer, changing in the policy would require changing the whole access control system.

Hence, thanks to our proposed OM-AM reference model, we believe that making a comparison or conflict between so called traditional access control models like RBAC and emergent access control technologies or standards like XACML, OAuth or UMA, or claiming that they are no more useful is a false idea. Actually, we can have a great collaboration and coordination between those different tools. Each tool plays its specific role within its specific layers working in a complementary way with each other, to satisfy different use cases. The work proposed in [36] using XACML in conjunction with OAuth 2.0 for scope definitions could be considered as a possible proof of concept of this idea.

In the following sections we discuss and overview the proposed solutions for IoT in the literature for each layer separately.

3. Review of the literature within the OM-AM model

In this section, a comprehensive review of access control solutions, in IoT, classified within the OM-AM model is provided. We first conduct a security requirements analysis to extract the Security & Privacy preserving (S&PP) objectives in IoT. Then we review the solutions presented in the literature, in each layer of our OM-AM reference model. Afterwards, we propose the following tax-

onomy, as depicted in Fig. 3, where each solution is categorized within the access control model and/or protocol it is based on.

3.1. Objective layer

This layer consists in constructing the security policy by studying the characteristics and features of the system to be secured and extract its main security requirements, then fixes the objectives to meet those requirements. Based on those objectives, (high-level) rules, according to which access control must be regulated, are identified. To meet this end, we conduct a Security & Privacy preserving (S&PP) analysis for IoT.

3.1.1. Security and privacy requirements in IoT

Actually, in order to build a suitable security mechanism for IoT, we need to understand the nature of applications and their security requirements properly. Then, it is mandatory, as a first step, to classify, on one hand, which domain application we are dealing with, and the various devices that comprise the domain application, on the other hand. Indeed, each domain application has specific characteristics and, thus, special security requirements that have to be taken into consideration to conceive a security solution, especially the access control framework. In addition, the classification of IoT devices will help to identify different security capabilities of the devices by assigning them a particular class. This will help in building an adequate access control framework guideline to achieve the required security level for each domain application. To meet this end, we list different application fields of IoT and specify the characteristics and security requirements of each field. Moreover, we briefly give a classification of devices in IoT.

IoT domain application taxonomy and their security requirements. IoT technologies can be applied in a variety of domains. However, it is impossible to envisage all potential IoT applications. A comprehensive survey about IoT applications could be found in [37]. In the present section, we examine the most popular IoT applications and identify their main characteristics and relevant security requirements. We categorize these applications into three domains: (1) Personal and home: at the scale of individual, home and healthcare. (2) Government and utilities: at the scale of community nation and region. And (3) Enterprise and industry: at the scale of industries and big companies. In order to consider the match between the application domain-specific requirements and the available access control technologies, the previous (S&PP) dimensions shall be analyzed, among which are:

- Confidentiality and integrity
- Reliability and Availability
- Privacy
- Usability

In the following, those dimensions will be used for considering the specific requirements of the three identified application domain categories:

Personal and home. In this field, IoT comes up with relevant services that improve our daily life style: In fact, the more physical objects and smart devices join the IOT realm, the more prevailing the impact and assets that IOT adds to our daily lives become. New and endless services can emerge to address society challenges and help people make better decisions. Healthcare applications like telehealth or telecare, or smart home applications are only some of the examples. The requirements for Personal and home domain applications are summarized in the following: **Integrity and confidentiality** are of great importance in such applications. In fact, IoT-related healthcare and home automation solutions, are expected to be closer by nature to user intimacy, and therefore their adoption depends on the level of their confidentiality and integrity. For example, Wearable computing devices MBAN: whereby the devices or sensors actively monitor the human body's vital signs (e.g., heartbeat, temperature and blood pressure) are dealing with very sensitive and private data. Therefore, any tentative of falsifying or disclosing patients data may cause fatal damages such as incorrect diagnosis or even death. Restricted access to the control of home devices and appliances are also necessary requirements. The need of **reliability and availability** depends on the type of the service provided. Indeed, In case of wellness services, occasional unavailability and/or failure may be tolerated. But, when the monitoring is a part of prevention, diagnosis, or treatment service, high-level of reliability and availability is critically required to ensure any urgent intervention in case of emergency. Then, efficient and Real-time data acquisition, event ordering, synchronization, and rapid response in emergency circumstances are crucial. As of **privacy**, users are directly and highly involved in such kind of applications since their personal data are considered as the fuel of all healthcare applications. Therefore, users have to take advantage of the available information/features that humans and their motion captures. As a result, access control model that are targeting this type of application are highly required to be user driven and privacy preserving. **Usability**: Healthcare and smart home services are expected to be used by the non-expert users. Since users may not be familiar with inner workings of security mechanisms, it is important that the system from user perspective be characterized as simple, transparent and inconspicuous. Therefore, preferred access control models are those which reduce user effort in system administration and facilitate more autonomous establishment of security context.

Government and utilities. For governments, IoT increasingly improves citizens standard lives while delivering cost saving to government. It boosts municipalities, utilities, federal agencies, and other public sector organizations to deliver smart services, and manage public infrastructure efficiently. Besides, it facilitates more intelligent decision making by aggregating vast amount of Big Data and improves collaboration and coordination among public sector agencies. IBM and Infor intelligent government are working together to provide intelligent city planning and operation software, embedded with analytics and mobile technologies – all available in the cloud to reduce fraud and simplify the citizen engagement process. We choose smart cities as example of this category. Actually, given a system, different subsystems are involved in Smart City areas. They are: Education, Public Safety, Transportation, Energy and Water, Government Services and smart buildings. The Security requirements for this category are summarized as follows: The major challenges in a smart city application, such as traffic monitoring, revolves around the **reliability** of the system in (i) the data sensing, and (ii) the data transfer both within the network of sensors but also to the external network (e.g., a traffic forecasting and management office). Here, the notion of reliability entails the **availability** and accuracy of sensors and their communication and system robustness, especially against the potentially adverse outdoors conditions. Furthermore, the age of collected/transmitted information is of high relevance, since in a real-time traffic estimation system the value of obtaining a measurement with a long delay is very small. For smart city networks, **confidentiality and integrity**are not the first requirement but they are still crucial because an outsider can induce information by correlating the results reported from multiple meters surrounding an individual. Moreover, because of the in-network data aggregation operations, data of different granularity and sensitivity with respect to the users privacy is being communicated and needs to be protected [38]. When personal data is collected by smart meters, smart phones,

connected plug-in hybrid electric vehicles, and other types of ubiquitous sensors, privacy becomes all the more important. In order to achieve user consent, trust, and acceptance of Smart Cities, integration of security and privacy preserving mechanisms must be a key concern of future research. The overall priority must be to establish user confidence in the upcoming technologies; otherwise users will hesitate to accept the services provided by Smart Cities [39]. Regarding **privacy**: end user is not involved in a potential way in all smart city applications. As a result, access control models designed for such scenarios are not highly required to be user driven. **Usability**: it will be crucial for the lift-off of the new smart city technologies to have user-centered applications and services that are relevant for ordinary consumers in their everyday life.

Enterprise and industries. For enterprises, IoT adduces positive business since new business models are created, and cost savings can be reached through management improvement, and optimization of equipment and resource usage. For industry, where IoT is also known as Industrial Internet of Things (IIoT), IIoT uses intelligent information technologies such as Big data analytics to fuel innovation. It has become a magic tool for big companies by opening new economic growth and competitiveness. IIoT is expected to boost, with unprecedented scale, speed and abilities, revenues by increasing production and creating new hybrid business models, and transform the workforce. We investigate smart grid application to illustrate the characteristics and security requirement of this category. The concept of smart grids includes multiple domains, ranging from the distributed power generation to the advanced metering infrastructure, including markets, retailers, transmission systems, distribution infrastructures, end consumers and so on. Some of those domains are under the umbrella of Critical Infrastructure Protection (CIP) and Critical Information Infrastructures Protection (CIIP) policies [40]. The security requirements for this category are analyzed as follows: Ensuring high **Reliability and Availability** in access to (and use) of information is a key aspect in a real-time system such as the Smart Grid, especially for the SCADA servers. Availability is critical for systems supporting grid automation, while it is less important in smart metering applications. Integrity and Confidentiality is the least critical dimension when considering grid automation systems and information, but a very important one for end consumers. Confidentiality is intrinsically linked to privacy aspects. Therefore, when we think about confidentiality in a smart grid, we should consider privacy of consumers, power market information [40]. Preserving authorized restrictions on information access and disclosure is mainly to protect personal privacy and proprietary information. This is in particular necessary to prevent unauthorized disclosure of information that is not open to the public and individuals. For **Privacy**: end user is not involved in potential way in all smart city applications. As a result, access control models designed for such scenario are not highly required to be user driven. For Privacy: end user is not involved in potential way in all smart city applications. As a result, access control models designed for such scenario are not highly required to be user driven. **Usability**: it will be crucial for the lift-off of new smart grid technologies to have user-centered applications and services that are relevant for ordinary consumers in their everyday life. The Smart Grid of the future should not be considered as an isolated technology. Instead, we should see it as a part of peoples overall life where innovative technologies should be a commodity in the background, while the rich user experience and usability should be in the foreground.

Devices taxonomy. To establish a solution that meets IoT requirements, we should define which category the IoT device belongs to. Since there is a large spectrum of IoT devices (e.g. RFID tags, beacons, sensor nodes, smart watches, smart phones and others), each device has specific capabilities, features and requirements. Authors in [41] and [12] have provided a detailed report on the miscellaneous properties of IoT devices. Actually, many ways have been already introduced in the literature to classify IoT devices. But we are interested in the one suggested in [42] based on spatial closeness of IoT devices to human (intimate, personal, social and public), using Edward Hall's theory of proxemics [43]. Indeed, from this classification, we can deduce that devices that are closer to human need an access control model that is more user-driven and that gives users full ability to control their intimate devices with their specific granularity. Contrariwise, devices that are classified as public do not need a fine-grained access control model. In addition, the involvement of end user in access control decision for this type of devices is not required.

In Table 2, we combine the results issued from analyzing domain characteristics and devices taxonomy.

3.1.2. Security & Privacy preserving (S&PP) objectives

Unlike other networking systems, new issues are raised, in term of security and privacy, in the area of IoT. Therefore, we propose the following P&SP objectives for analyzing Privacy and Security in IoT. These criteria are based on extensive review of the literature and the recent published European Union (EU) regulation for electronic identification (eIDAS) [46]

- **Privacy**: is the ability of an entity to determine whether, when, and to whom personal information can be released or disclosed [47]. An access control system should preserve its users' privacy, which is one of the ways to gain user trust. User privacy including user data and personal information should be flexibly preserved according to the policy and expectation of IoT users. We quantify this objective trough the following key factors shaping privacy: (1) **Transparency**: consists in helping people to understand who knows what about them, how their data will be used, with whom it is shared and how long it is held. (2) **User-driven**: users are the master of their own data, they have full and granular access control over the data they share in the network or in the cloud. (3) **Anonymity**: IoT applications are required to not disclose the identity of their users. (4) **Pseudonymity**: trades off anonymity with accountability. Actually, actions of a person are linked with a pseudonym, a random identifier, rather than an identity. Pseudonymity might be used to serve many purposes [48], especially resolving privacy and accountability concerns in the IoT. (5) **Unlikability**: qualifies pseudonymity in the sense that specific actions of the same person should not be linked together. This requirement might serve as a protection from profiling in IoT. (6) **Unobservability**: ensures that a user may use a resource or service without others, especially third parties, being able to observe that the resource or service is being used [49]. It requires that users and/or subjects cannot determine whether an operation is being performed. (7) **Decentralization**: Each node in the network shares its data with others nodes directly, without intervention of any third or trusted entity.
- **Technologies constraints**: (1) **Flexibility**: access control should be flexible to be adapted to different contexts. Furthermore, it should support long-lived and planned patterns as well as causal spontaneous and short-lived interaction. Indeed, the collaboration between users is established in unscripted way and the role of service provider or service consumer can no longer be static or identified a priori, since it can be played alternatively by the same entity. (2) **Scalability**: IoT is a more demanding environment in terms of scalability and manageability. Due to the potentially unbounded number of things (resources and subjects), access control mechanism should be extensible in size, structure, and number of users and resources.

Table 2
Security requirements and device taxonomy of IoT applications domains.

Domain application		Devices proximity	Reliability & availability	Confidentiality & integrity	Usability
Personal and Home	Healthcare	Intimate Personal	Highly required [44]	Highly required	Highly required
		Intimate	Temporal unavailability is tolerated		
	SmartHome	Personal	High reliability for (home security and home automation)	Highly required	Highly required
		Social	Low reliability for media and entertainment		
Government and utilities	SmartCity	Personal			
		Social	Not highly required [45]	Not highly required except for user's private data [38,39]	Preferred
		Public			
Enterprise and industry	SmartGrid	Personal			
		Social	Highly critical	Not highly required except for consumer's private data	Preferred
		Public			

(3) **Lightweight**: access control, designed for IoT, should support lightweight solutions and standards, due to the low capabilities of power, memory and computing of IoT devices meaning that all introduced security mechanisms shall be designed such that the total overhead due to computation and communication is as low as possible on the device side . (4) **Heterogeneity**: is a key challenge in IoT. Actually, a collaborative environment may combine several technologies and different devices and ecosystems. They may be conceived by diverse constructors and are thought up for diverse purposes and designed for different application domains, making it arduous to achieve a global agreement or adopt any specification.

- **Social & Economic aspect of IoT**: there are several Social & Economic challenges that need to be addressed: (1) Interoperability/cooperativity and collaboration: IoT is an ecosystem that requires, in one hand, the collaboration between a plethora of untruthful stakeholders establishing loose relationships, such as individuals, public and private establishment. In other hand, it establishes communication and information exchange across heterogeneous set of devices. Thus, access control model must be designed for multiple organizations. Each of them sets up its own policies and must respect other collaborating organizations policies. (7) Context awareness: The context is particularly important in IoT. It provides services and applications that use knowledge and inspire its intelligence from its surrounding contextual information about user and his environment. Actually, in IoT, sensors continuously generate enormous amounts of raw data and context-aware computing has proven its efficiency to understand this data and add value to it.
- **Confidentiality and integrity:** confidentiality means no unauthorized disclosure of resources and integrity means no improper modifications of resources. Moreover, access control system should have the following features: (9) high Granularity: which means expressiveness of the grammar used to formulate access control rules: the more flexible the grammar is and the more information it can cater for, the more fine-grained the resulting access control will be. (10) Revocation: the ability to revoke permission to access resources and make sure the revoked user cannot access the associated resources anymore. (11) Delegation: a subject can grant access rights or part of the granted rights to another subject. As many things are owned by their users (either permanently or temporarily) and may belong to a group it is necessary to consider the design of delegation mechanisms.
- **Reliability and availability:** the continuity of service leads to reliability while the readiness for usage leads to availability. In the IoT context, such properties may also be declined to (1) Offline mode: decisions are made even if their maker (that could be resource owner) is absent or not connected. (2) Short-term availability: the IoT resources must be available to authorized users with reasonable response-time as process or data may have timeliness constraints. (3) Long time availability: regulations impose that some data must be kept for a very long time (e.g., cancer records must be kept for the patient's lifetime, and records of genetic diseases have to be kept even longer. Only some well-identified users should have the ability to delete those data, and only after the appropriate time period has expired.
- **Usability**: access control should be easily managed, expressed and modified. Indeed, with the omnipresence of IoT devices that encompass every day and personal tools such as toothbrush, fridge, wearable, etc. Users, with different expertise, are more involved nowadays in authorization activities than in the past.

A comprehensive and holistic access control framework for IoT requires that all above objectives, summarized in Fig. 1, would be achieved.

3.1.3. *Summary*

We can deduce from our previous analysis that IoT applications will need to be built on principles of cooperation and collaboration, openness/interoperability, high scalability, flexibility and distribution. We can conclude that in personal and home category that encompasses smart home and healthcare applications, end user is considered as a pivot element due to its high involvement. As a result, access control models targeting such domains are required to be more user-driven. They should allow end user to have full control over his own resources. In the government utilities, enterprise & industry, end user involvement is less important than in the first category. Fig. 2 illustrates our findings.

It is unlikely that a one-size-fits-all approach in all IoT applications works, but rather many and diverse approaches. A peruse-case specific vulnerability analysis will identify the level of security required for each device in certain applications and which access control solution achieves the required level. However, the common requirements for all IoT applications are: high flexibility, scalability, heterogeneity, collaboration between different stakeholders, and the need of lightweight security mechanisms due the omnipresence of constrained devices in all IoT application domains. Without appropriate security mechanisms, attackers might gain control over things and put our lives in danger.

To bridge the policies and the actual mechanisms to enforce them, an access model or more precisely an authorization model is needed.

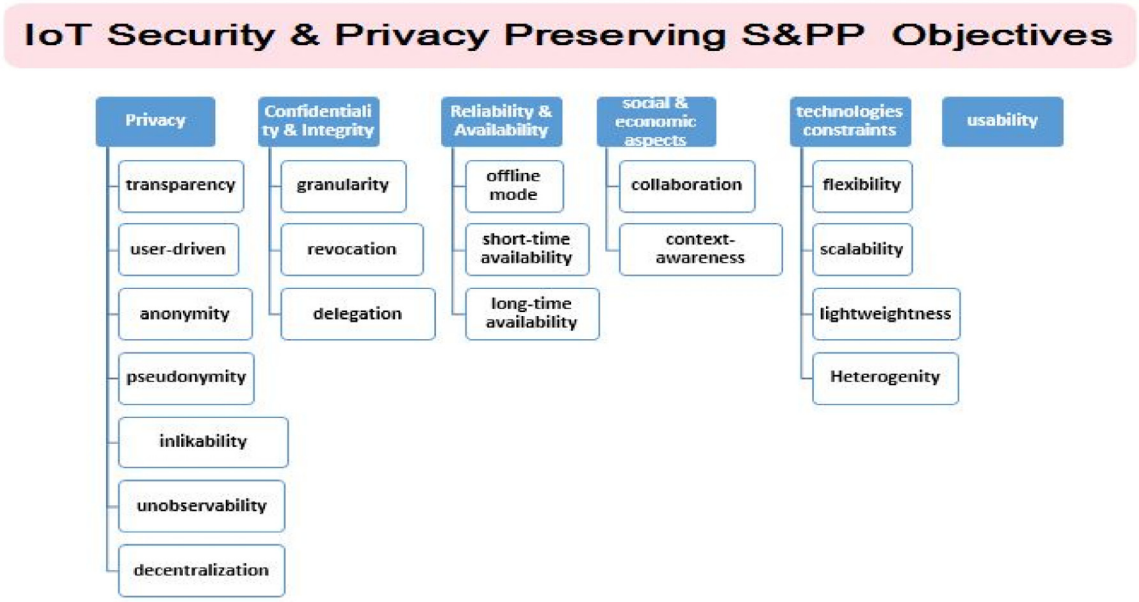


Fig. 1. IoT Security & Privacy preserving (S&PP) objectives.

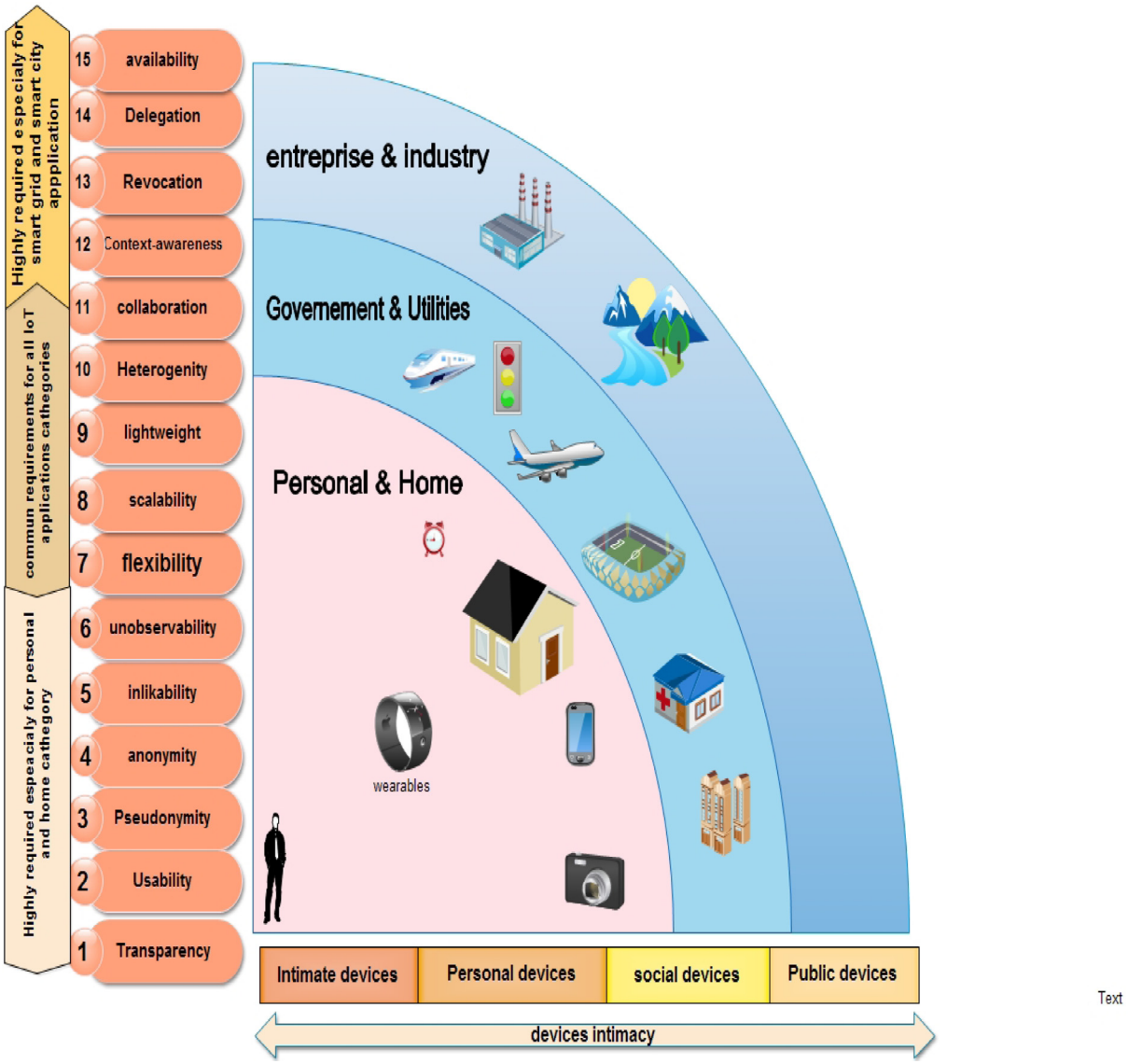


Fig. 2. IoT domain application taxonomy and their security requirements.

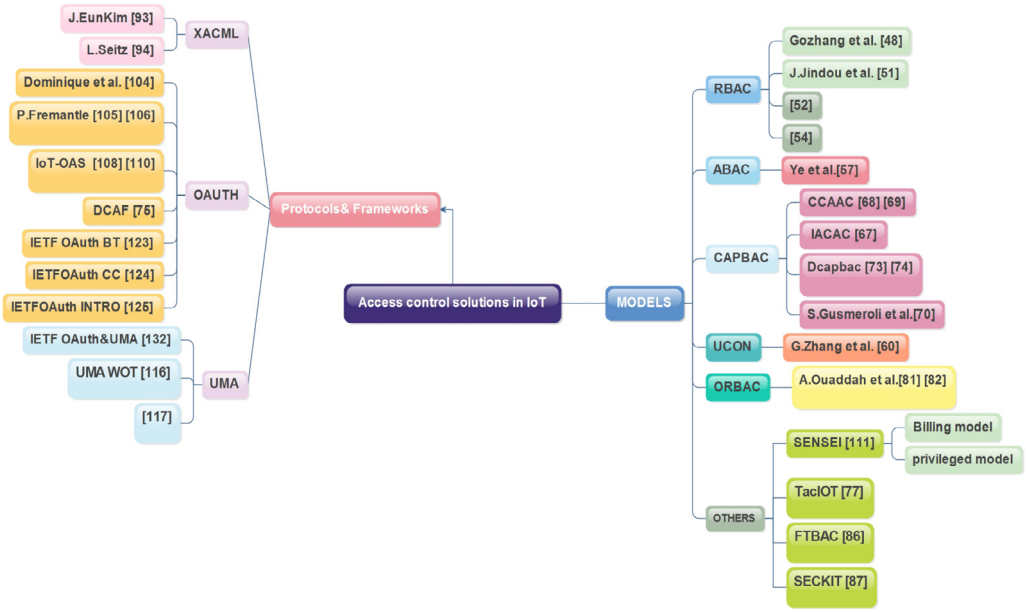


Fig. 3. A taxonomy of related work.

3.2. Authorization model layer

Many access control models have been proposed in the literature to address security issues in IoT. We cite below the most recent and relevant ones.

3.2.1. Access control solution based on RBAC model

RBAC (Role-Based Access Control) [20] is an access control model and framework for controlling user access to resources based on roles. This model consists of four different components and each one of them assigns to RBAC a number of functionalities. These components are the core RBAC, the hierarchical RBAC, the static separation of duty relations and the dynamic separation of duty relations. The core RBAC model is composed of five static elements. These elements are the users, roles, and permissions, with the latter being composed of operations applied on objects. The relationship among the elements of the core model is straight forward many to many. Roles are assigned to users and permissions are assigned to roles. Moreover, we identify two distinct phases in RBAC. The first is the design where a system administrator can define a number of assignments between the elements in the computer system. The second the run-time phase where the assignments in the system are enforced by the model as it is specified by the security policy of the system, which was prescribed during the design phase.

More of RBACs virtues are the support of important principles, namely the least privilege, separation of administrative functions and separation of duties [15]. However pure RBAC model is inappropriate to model security policies that interpret complex and ambiguous IoT scenarios. It must be extended to face the previous mentioned challenges. We list below different propositions from the literature aiming to extend RBAC in IoT environments:

Authors in [50] adopt a service-based approach to release IoT [51,52], where each IoT device should offer its functionality as standard services. Then, the service is considered as the target of the request, whose authorization is verified by access control before being performed by the service. In order to take contextual information, such as time, location, state of the environment in access control decisions, authors extended the RBAC model by the introduction of context constraint collected from the environment of the physical object. The web service technology provides great interoperability between heterogeneous devices. However, authors did not clearly describe how the physical object is mapped to one or more web services and more importantly they did not describe how the contextual information is collected from the physical object environment to be included in the authorization process especially in a real-time manner. This makes their proposed solution seem to be more suitable for designing context-aware access control model in web services rather than in IoT environment. Actually, they have considered only IoT users rather than devices. The role of smart objects in making access decision is completely annihilated. Furthermore, the presented model has been only demonstrated through use case studies rather than implementation.

Similar to the previous work, authors in [53] adopt the web of things (WoT) approach and the RBAC model as a basis to conceive an access control method to enhance device security and privacy. However, unlike [50], they did not extend RBAC with contextual constraints to fit IoT, but they rather propose a role-based access control model that integrates Social Network Services (SNS) such as Facebook to enable owners to leverage user profiles and social links in existing social networks to create policies for access control on devices. Through an in-depth analysis of SNS, user data and abstraction of RESTful Web service application interface (API), they redefined the user (U), role (R) and permission (P) sets of RBAC model as well as the mapping between these sets. Providers, which are the devices owners, can define user-role assignment policy according to user profiles (e.g. age, gender, university) and social links (e.g. close friends, family, etc), and permission-role assignment policy according to device attributes (e.g. title, tags, type, location, and status). As authors claimed, using social networks enables users to share devices with people they know and trust and manage access to their resources in a user-friendly and customary way. While the integration of network service (SNS) puts forward this work to be characterized by high usability and user-driven feature, the proposed method cannot satisfy all access control requirement in IoT. Actually, the device-to-device communication is not considered. Moreover, the use of SNS data as basis to create access control policies over devices makes the proposed solution strongly tied to SNS. Resource owners and requesters must have an SNS profile or account to interact with each other. This, in one hand, obviously increases the dependency of users on social network services and on another hand, introduces the social network

service provider as an implicit trusted third party. For those reasons, we think that more privacy preserving mechanisms are required to protect user's access control policies from malicious acts of service providers.

A close proposal to [50] is presented in [54], where RBAC model is integrated into the Web of Things (WoT) approach to specify access control to the physical things that are accessed and controlled via the Web. For the purpose of this integration, authors provide a careful mapping between the entities of RBAC that are: User/Subjects, Permissions/Rights, Objects, Authorization Rules Session and components of the WoT. However, the mapping of the role notion in WoT is not clearly identified. Authors point out two most critical issues in using RBAC for enforcing the specified access policies in WoT environment, that are the use of the concept of a reference monitor (RM) and role proliferation. To address those issues, they leverage the concept of role parameterization, developed by [55], to deal with the issue of role proliferation and propose a conceptual structure of RBAC/WoT access control domains, based on the reference monitor where the role-based access control is incorporated to handle the pre-decision authorization rule. The proposed architecture is based on a central Access Control Decision Facility (ADF), which adheres to the RBAC policy decision of whether to grant or reject the authorization request. Therefore, when the entity tries to access a WoT resource, the request is intercepted by an Access Control Enforcement Facility (AEF) entity. Before making any decisions, the AEF forwards the request to the Access Control Decision Facility (ADF). Hence, this approach is completely centralized where all access control logic is externalized into the (ADF). Thereby, end-devices (i.e., sensors, actuators) play a limited role as simple information providers. Furthermore, authors claim that traditional access control models such as DAC and MAC focus on the protection of data in closed environments and are not sufficient in isolation for providing security for a large-scale, distributed and sometimes resource constrained pervasive environment like in WoT context. Hence, their approach utilizes RBAC to control access to things on the Web. However, we think that the RBAC itself shows inappropriate aspects in a distributed network environment. Second, no lightweight mechanism is proposed to make RBAC supported by constrained devices. The RBAC-based authorization model is again adopted in [56] using the things particular role(s) and application(s) in the associated IoT network. The authors focus more on the establishment of an authentication protocol based on the OpenID [57] technology, trustable central entities, and an efficient secure key establishment through ECC (Elliptic Curve Cryptosystem). However, the authorization process is slightly described in this paper. Actually, only a general overview of RBAC model is given. The authors neither describe the security policy nor how the role of IoT things is identified or assigned and more importantly they did not justify the fitness or adaptability of RBAC in IoT context. Furthermore, several security gaps of this work are discussed in [57]. Therefore, authors in [57] provide enhancement to the protocol to fill the discovered weakness gaps. The improved protocol facilitates many services to the users such as user anonymity, mutual authentication, and secure session key establishment. Finally, the performance and security analysis reveals that the improved protocol presents many advantages against popular attacks, and achieves better efficiency at low communication cost.

3.2.2. Access control solutions based on Attribute-Based Access Control (ABAC) model

In ABAC model, access is granted according to attributes presented by a subject. Actually, the subject and the object both identify through the attributes associated with characteristics [24,58]. ABAC is composed of two aspects: the policy model (sometimes referred as PBAC: Policy Based AC) and architecture model which applies the policy. The basic ABAC model asserts that access can be determined based on various attributes presented by a subject. Policy rules specify conditions under which access is granted or denied. In ABAC model, the subject and the object all identify through the attributes associated with characteristics. The user is granted appropriate access permissions to the system according to his attributes when he initiates an access request.

Much work has been done in the literature using ABAC model in IoT:

More recently Ye et al. [59] have proposed an efficient authentication and access control scheme for the perception layer of the Internet of Things. The ABAC-based authorization method has been adopted as access control policy and a simple and efficient mutual authentication based on secure key establishment based on ECC. The described protocol provides much lower storage and communication overheads to solve constraints in resources of the IoT perception layer. Accessing the data on the basis of user attribute certificates in the access control authority ensures fine-grained access control. However, it requires complex management and impedes its deployment to constrained devices. Consequently, they only provide theoretical results of the proposed model.

3.2.3. Access control solutions based on usage control (UCON) model

The usage control (UCON) proposed by [26–28] model is considered as the next generation of access control models. It introduces various novelties compared to traditional access control such as RBAC and ABAC. It handles the problem of authorization in a continuous way before the access execution, during the execution and afterwards. Moreover, it supports mutability of attribute, meaning that if access attributes are changed while the access is in progress and this change leads to unsatisfaction of the security policy, the granted access is revoked and the usage is cancelled. More details about UCON model are given in [60] . Research has also been conducted to use UCON in collaborative systems [61]. The UCONABC model, which consists of eight components, subject attributes, objects, object attributes, rights, authorizations, obligations and conditions. The notion of subjects and objects as well as the association with their attributes is straightforward. A subject can be an entity in a system and its definition, as well as its representation, is given by a number of properties or capabilities in the associated subjects attributes. Each object can be associated with object attributes. Subjects can hold rights on objects. Through these rights, a subject can be granted access or usage of an object. It is worth mentioning that both subject and object attributes can be mutable. This means that the value can be modified only by an administrative action and not by its users activity.

It should be noted that, at the state of the art, the only work that has stressed the particularity of UCON model over traditional access control model such as DAC, MAC and RBAC, that makes UCON more suitable to meet the dynamic nature of IoT was presented in [62]. This particularity resides in the concept of continuity of decision and mutability of attributes introduced by UCON model. A mapping of UCON abstractions and IoT entities is proposed as follow: The subject(S) of UCON in IoT is the Device (D) such as cars. The attribute(S) of UCON in IoT is the Att(Device), which contains the information about the trust value of the device and so on. The subject(O) of UCON in IoT is the Service(S), which lays in the application layer and requests the service information provided by the services located in the wireless sensor network. The attribute(O) of UCON in IoT is the Att(Service), which contains the service information such as the digital sources for the car and so on. The condition(C) of UCON in IoT is decided by the policies according to the wireless sensor network, such as the trust value and other decision factors. The condition(C) is the constraint according to the actual situation in a wireless sensor network, such as limits of geographical location. The oBligation(B) of UCON in IoT

is according to the needs of the wireless sensor network. The obligation of the device should be do ne before or during the usage control in IoT. The Authorization (A) of UCON in IOT is set by the needs of usage control, and decided by the device and the service. The usage decision for the access control is made between the Device and the Service according to certain access control policies, using the Device's trust degree and the Service's trust threshold and some other information. The assessment model is based on a fuzzy theory. Although some theoretical experiments are introduced, the practical feasibility of this approach is not demonstrated.

3.2.4. Access control solution based on capability-based access control (CapBAC) model

Capability-based access control (CapBAC) is based on the concept of capability that contains rights granted to the entity holding it. The concept of capability was introduced in [63] as token, ticket, or key that gives the possessor permission to access an entity or object in a computer system.

Traditionally, discretionary access control, first proposed by Lampson [64] was represented by Access Control Matrix (ACM), whose column basically describes a list of objects or resources to be accessed, and whose row represents a list of subjects or whoever wants to access the resource. From this ACM, two traditional access control models co-exist: Access Control List (ACL) and capability-based access control. Many comparisons have been made by many scientists [65,66] between ACL and capability-based access control where many security threats and especially the confused deputy problem were identified in ACL while it is not the case in the capability-based access control. Actually, ACL is centralized by nature, cannot support different levels of granularity, is not scalable and is prone to single point of failure. The capability-based access control (CapBAC) is based on the concept of capability that contains rights granted to the entity holding it. The concept of capability was introduced in [63] as a token, ticket, or key that gives the possessor permission to access an entity or object in a computer system. Actually, CapBAC has been adopted in many large scale projects [67] and has been widely used in the IoT field. However, applying the original concept of capability based model into access control model as it is to IoT, has raised several drawbacks. The capability propagation and revocation are two major drawbacks of classical capability based model that has been pointed out by Gong in [68]. He proposed a so-called Secure Identity-based Capability System (ICAP) as a solution to the identified challenges. The ICAP [68] aims basically to extend the capability system concept, in which any user or subject that wants to get access to a certain device or resource uses a capability. Access is granted only if the capability presented by the subject matches with the capability stored in the device or an entity that manages the device. The particularity that ICAP introduced over classical capability based system consists in including the identity of subject or user in its operation. In this way, ICAP claims to provide more efficient control in capability propagation and offers more scalability by reducing the number of capabilities stored in the so-called "Object Server", "Gateway" or "Access Point". The ICAP structure and how capability is used for access control is represented as ICAP = (ID,AR, Rnd) where ID presents the device identifier, AR the set of access rights for the device with device identifier as ID, and Rnd the random number to prevent forgery and it is a result of one-way hash function. However, Gong [68] did not clearly describe the security policy used in the capability creation and propagation. Including context information in making access control decision upon an access request from a subject or user was not considered either. The same model introduced in [68] was adopted by Mahalle in [69]. Its novelty resides in the fact that it presents an integrated approach to authentication and access control based on ICAP for IoT. The proposed model is called the Identity Authentication and capability-based Access Control (IACAC) model. In IACAC, devices are connected with each other through the use of an access point and then the capability-based access is allowed to the other device through Capability based Access Control (CAC). Each established communication is verified by its capability access. Only after the capability verification, the devices are able to communicate with each other. Any device which wants to communicate with another device is able to initiate the communication by sending the request to a specific device. The second stage is to verify whether that requesting device is having the capability to communicate with called device. This access right gets checked using the capability of that device which is associated with every device. Furthermore, a modeling of three attacks investigated in the paper was presented. Its suitability to the following parameters: scalability, granularity delegation, and efficiency time security is discussed. Moreover, a mathematical model for improving queuing analysis of IACAC is presented.

The proposed model uses a public key approach and is compatible with the lightweight, mobile, distributed, and computationally limited nature of IoT devices plus existing access technologies like Bluetooth, 4G, WiMax, and Wi-Fi. IACAC is implemented in a Wi-Fi environment and evaluated by the Automated Validation of Internet Security Protocols and Applications (AVISPA). The performance analysis of the protocol in terms of computational time compared to other existing solutions is discussed. However, the specification, as well as security evaluation of the CAC propagation and revocation, was left unaddressed. Another interesting but missing aspect for IoT will be to define a lightweight version of CAC for resource constrained devices in IoT like sensor nodes. Efficient interoperability is still an open issue in this work.

Another extension to (ICAP) model [68] to support the context awareness in federated IoT is presented in [70] and [71]. Researchers presented an access delegation method with security considerations based on Capability-based Context-Aware Access Control (CCAAC) model intended for federated IoT networks. An additional field called Contexts (C), which contains context information related to the capability, is added in the extCAP. By including this field, the external capability structure in CCAAC is defined as extCAPi = (O,AR, C, Rndi), where O is the Name of object or resource to be accessed. AR is a type of access right, e.g. read, write, execute, C is Context information and Rnd is a random number generated from a one-way hash function to prevent forgery. CCAAC is claimed to be a special case of UCON where capabilities are modeled as subjects and objects attributes, and can be propagated through mutable attributes. Both these works focus on the security requirements in isolation. Actually, the approach used in this paper requires that an additional trusted by both domains entity be involved in the design. However, not all IoT scenarios consider that a prior knowledge of the trust relationship between two network domains in federated IoT is established.

The work in [72] is a part of IoT@Work project [73]. The capability-based access control (CapBAC) model is extracted from the one proposed by Skinner [74] in the project: SUN DIGITAL ECOSYSTEM ENVIRONMENT. The proposed framework adopts a centralized approach for managing access control. It defines a central policy decision point (PDP), implemented in a non-constrained machine, responsible for the management of authorization decisions. However, we notice that this work deals with IoT as a usual computing platform. As a result, its special characteristics, such as lightness and smartness in device side are neglected.

A close approach to [72] is adopted in [75], but this time, the capability model was directly implemented on resource-constrained devices, within a distributed security approach. Actually, authors have given in [76] an overview of three approaches to implement access control model in IoT: the centralized approach,

centralized and contextual approach and the decentralized one. The advantages and drawbacks of each one were provided. The authorization logic is embedded into device side thanks to the use of lightweight technologies such as JavaScript Object Notation (JSON) as a representation format for the token and emerging communication protocols such as CoAP [77] and 6LoWPAN [78] as well as a set of cryptographic optimizations for ECC. Even though DCapBAC model presents interesting features regarding scalability, interoperability and considers devices as smart objects able to take autonomous decisions, with authorization logic, it lacks granularity and context-awareness. Moreover, DCapBAC focuses more on the authorization enforcement stage, while nor the beginning of access control procedure neither the capability token generation procedure are investigated. These last issues are addressed by authors in another paper [79] where a flexible trust-aware access control system for IoT (TACIoT) that extends DCapbac is proposed. This proposed solution will be discussed in this paper in Section 3.2.6. It is worth to note that the work in [75] is a promising solution for IoT that is able to guarantee the possibility to embed a notable part of access control logic in device side. Note that finding equilibrium between end device autonomy to control access overproduced information and the computing efforts requested by the access control mechanisms themselves is still an open issue. Some efforts have already been done to define proper protocols for the specification of access control policies in IoT, but a standard which addresses specifically IoT paradigm is still missing. This dilemma of centralized and decentralized approaches will be extensively highlighted in this paper in Section 5.2.

3.2.5. Access control solution based on Organizational-Based Access Control (OrBAC) model

The OrBAC [80] model is conceived to address existing issues in extended RBAC models. It introduces the notion of "organizational" as a new dimension, and separates between the concrete level (user, object, action) and the abstract level (roles, views, activities). This model includes different context data which can be historic, spatial, and temporal or declared by the user. If we can assume that OrBAC provides a framework for expressing the security policies of several organizations, it is unfortunately only adapted to centralized structures and does not cover the distribution, heterogeneity, collaboration and interoperability needs. Multi-OrBAC [81] is an extension of the OrBAC model designed for multi-organizational. The main defect of Multi-OrBAC lies in the fact that the definition of the security policy of each organization must take into account the entities belonging to other organizations, and therefore requires mutual trust between organizations regarding the management of these entities. Poly-OrBAC [82] overcomes this problem by integrating the OrBAC model to represent the internal policies of each organization and web services technology to ensure interoperability between organizations. However, technologies used in PolyOrBAC such as SOA-based web-services are not supported by IoT constrained devices. In this direction, SmartOrBAC [83] and [84] aim to extend OrBAC model in IoT environments. The main contribution of this work consists in enhancing the "context" notion (originally present in OrBAC) in order to fit the IoT requirements. However, no lightweight mechanisms are stressed to reduce the complexity of OrBAC model to be supported by constraints devices.

3.2.6. Access control based on other models

SENSEI [85] is a large scale project, which has been developed as part of the European ICT-FP7 SENSEI [85–87]. SENSEI developed an overall authentication, authorization and accounting framework. The SENSEI AAA architecture relies on a number of advanced concepts: trust management, security management, scalability for identity management, privacy analysis and privacy preserving reputation establishment. SENSEI offers two approaches of access control model:

(1) Billing-based access control (based on the commercial trust model): the access control decision is business model driven, i.e. the identity of the user does not matter and the service can be provided to anyone as long as an adequate reward is provided.

(2) privilege-based access control: (based on the corporate trust model): the decision is organizational policy based, i.e. the identity of the user is significant and the service being provided has some inherent security sensitivity meaning to the organization(s) involved and should only be provided to certain users.

Access control and trust are closely related notions as the level of access granted by a particular device to another device depends on the level of trust between these devices. The same idea emerged in [88]. Authors in this paper propose to use the trust as a tool in the decision making of access control based on a Fuzzy approach where fuzzy trust values are mapped to access permissions to achieve access control in IoT. The trusts values are calculated by the FTBAC framework from factors like experience (EX), knowledge (KN) and recommendation (RC). Based on these collected parameters, the proposed FTBAC framework calculates the trust score. For the calculation of trust score, the linguistic values of experience, knowledge and recommendation are used. This trust score is then mapped to access permissions for providing access to the resources or devices with the principle of least privilege. For example, if the fuzzy trust value is T1 = Low which is a dependent parameter on EX, KN and RC, then the corresponding access right AR is and if T2 = Average, then the AR is (READ), FTBAC scheme is simulated and results show that it can be used to calculate fuzzy trust values for any number of devices which makes it more suitable for scalable IoT, real implementation and integration with an adequate access control model is still missing.

In [79], authors presented another trust model based on fuzzy logic called TACIoT. Such model follows a multidimensional approach to enable an accurate trust value computation for IoT devices. In particular, in contrast to previous models that usually only consider reputation and feedback, the model takes into account four dimensions: reputation, quality of service, the social relationship between IoT devices as well as security aspects. These parameters are then used by smart objects to drive their access control logic. Furthermore, the proposed trust model has been integrated into a lightweight and flexible access control mechanism based on DCapBAC [75], with the aim of making IoT devices aware of other devices' trust scores and drive their access control decisions accordingly. This model has been implemented by the Trust Manager and then integrated with this IoT security framework [136], which is based on the Architectural Reference Model [137] (ARM) from IoT-A EU project. The feasibility of TACIoT was demonstrated by testing the software implementation on real scenarios for constrained and non-constrained devices. (TACIoT) provides an end-to-end and reliable security mechanism for IoT devices, based on a lightweight authorization mechanism and a novel trust model that has been specially designed for IoT environments. Nonetheless, the definition of a fully distributed approach and the introduction of a well-defined trust negotiation language supporting the semantic interoperability of IoT context is still missing, as confirmed in the two recent surveys on trust in IoT provided in [10] and [6].

Another work [89] proposes a sophisticated model-based Security Toolkit named SecKit. It is integrated in a management framework for IoT devices called iCore Framework [90]. It provides the specification and enforcement of usage control policy including authorizations and obligations to enable the protection of user data. The usage is regulated through profiles. Profiles consist in defining the conditions, specified in form of sets of security policy configuration rules, under which a set of enforcement policy templates should be activated. For example, a profile can be specified to re-

strict the amount of user information accessible to the IoT devices (enforcement) when the user is in a public space that is considered to be a potentially unsafe situation (configuration). The specification of authorization and obligation policy rules is done in SecKit using an event-based Rule model containing Rule Templates. Events represent actual or tentative events which mean respectively activities in the IoT system that already took place or are about to take place but have not yet started. The specification of detective and preventive policy rule templates is enabled through the distinction between actual and tentative events. Detective rule templates are only able to react to actual events and execute additional compensation actions while preventive rule templates may allow, deny, modify, or delay the execution of tentative activities. The SecKit foundation is a collection of meta-models that describes Data, Time, Identity, Role, Structure, Behavior, Trust, Rule, and Risk. A part of the model-based Security Toolkit (SecKit) [89] has been implemented as an extension to the open source broker mosquito in [91], where the design, implementation and evaluation of enforcement of security policy rules with the Message Queue Telemetry Transport (MQTT) protocol [92] is proposed. The performance results are promising; complex security policies are enforced with a very small additional delay of 10 ms in contrast to the normal operation of the broker. It is available as open source software for download at: https://github.com/r-neisse/Release. While the SecKit is considered to be a powerful tool to express granular access control policies, the generation of many different profiles and different versions make the framework extremely complex to handle and maintain. Actually, the complexity to use the framework is highly bounded to the complexity of the environment where the user is active. While such complexity cannot be avoided, the framework aims to enhance its usability by providing an engineering tool [93] (i.e., the SecKit itself), that automates the choices for the user.

3.3. Architecture layer

So far, we reviewed the proposed models in IoT. In this subsection, we sketch different authorization architectural solutions existing in IoT field

3.3.1. ***Extensible Access Control Markup Language (XACML) standard***

XACML [21] is an XML-based language for access control (authorization) that has been standardized by OASIS (Organization for the Advancement of Structured Information Standards). It describes both an access control policy language (ABAC) and access control decisions (request/response). A comprehensive study on XACML has been done in [94].

Kim et al. [95] proposes an extensible (Open Services Gateway initiative) OSGi-based architecture for highly heterogeneous smart home systems to enable dynamic integration of devices and services. The policy model maps a user role to permissions on a device with a collection of attributes. The smart home policy model represents fine-grained access policies similar to the ones enforced in real life. However, this proposal is bound to the use of XACML, which is not specifically designed for use in constrained devices. Furthermore, the device to device communication is not considered. In this direction, another generic authorization Framework for the Internet-of-Things is proposed in [96]. It supports fine-grained and flexible access control for any objects with low power and memory resources. Based on current Internet standards and access control solutions such as XACML and Security Assertion Markup Language (SAML) [97], the decision of access control is enforced locally by the object (local PEP) taking its local parameters into consideration. Local decisions are enabled via XACML obligation. Due to the complexity of XACML policy evaluation for objects with high resource constraints, a great part of the decision-making process for granting access is externalized (externalized PDP). Despite the verbosity feature of XACML, Seitz's solution faces this drawback by proposing compact representation in JSON for assertion format. Nonetheless, the solution is still too heavy to be embedded in device side. As a result, a great part of the decision-making process for granting access is externalized (externalized PDP) and the object simply enforces the execution of the authorization to take into account the local decision that justifies the level of distribution and lightness of XACML-based solutions. In [70], authors had adopted ABAC model as it is, without any extensions to IoT context. The solution offers, in fact, great granularity and context awareness, but seems too heavy and complex to implement in constrained devices and get it managed by ordinary people. This explains the very low level of heterogeneity, usability, and lightness of the solution.

3.3.2. *Access control solutions based on Open Authorization (OAuth) protocol*

OAuth is an access control framework for clients accessing resources on Web servers. It has gained a lot of attention recently. The OAuth 1.0 Protocol [98] and its successor, the OAuth 2.0 Framework [22] were designed to address the issues of privacy and access control related to large-scale Internet connected applications. It is an authorization framework which enables users to grant third party applications, acting as relying party (RP), access to the protected resources (hosted at particular service playing the role of an identity provider (IdP)) without revealing their login credentials to the third party. A comprehensive survey about OAUTH could be found in [99]. There are already over one billion OAuth-based user accounts provided by major service providers such as Facebook [100], Google [101] and Microsoft [102].

In fact, much effort is already in progress in many research projects to implement OAuth over IoT protocols, such as COAP in [103], MQTT [92] in [92], and BACNET [104] in Building as a service Project [105].

Dominique Guinard proposed Social Access Controller (SAC) [106] as a user-centric solution that enables users to share with other users access to their devices. It relies on functionality provided by popular social networking sites to authenticate users, advertise and discover devices. It is based on OAUTH 1.0 as access control protocol. Then SAC requires from the devices owners to manually configure the permissions of each device for every user he wants to share data with. This model is useful when the number of devices and friends is small but becomes quite unmanageable (for the owner) when this number grows up. The core idea is to leverage existing online social structures rather than rely on closed databases of credentials. Thus, the SAC architecture provides a framework which is built upon fast growing social networks, such as Facebook, Twitter or LinkedIn, to allow users to share physical objects with actual friends, relatives or colleagues.

The work in [107] was the first to implement OAuth2 with MQTT. Actually, authors explored the feasibility and effectiveness to use OAuth2 as part of the MQTT protocol flow and within an MQTT broker to make federated, user-directed access control decisions in IoT system. As proof of concept, a prototype that uses OAuth 2.0 to enable access control to information distributed via MQTT was built. The results of this prototyping activity were evaluated, and the strengths and weaknesses of this approach were identified. While there were some issues with implementing Federated Identity and Access Management (FIAM) for IoT using OAuth2 with MQTT, the benefits of building on existing widely implemented and deployed protocols are significant. Many years of work and review have gone into the security of OAuth2, and from this work, we can state that it is possible to re-use this work with IoT devices and new protocols. However, issues like usage

control, simplicity of key issuing, developer portals are missing in this paper. To tackle those aforementioned problems, authors address in a recent work [108] the problem of adapting the principles and technologies of Web API management to IoT and implement a prototype which is the first of its kind to add support for IoT-specific protocols to API management systems. Moreover, the prototype demonstrates the use of an extension to the OAuth2 protocol called Dynamic Client Registration (DCR) [109] as a means of ensuring the uniqueness of tokens stored on hardware. However, the adopted approach in both works is completely centralized and not user driven.

Another project proposes in [104] an addendum to the BACnet standard, using OAuth 2.0 as access control mechanism. Another extension of BACnet, the BACnet Internet Transport Binding (ITB) that is currently being specified will also use OAuth 2.0 for secure authorization. This demonstrates that OAuth is considered to be suitable for the WoT in general and Web-based Building Automation Systems in particular. As OAuth has also been adopted by extensions to the BACnet, it seems to be a reasonable choice for the BaaS project as well. This is emphasized by the fact that the combination of OAuth and the CoAP protocol has already been investigated. A novel architecture with a generic and external authorization service based on OAuth targeting both internet and IoT scenarios have been presented in [110]. The design goal of the proposed architecture is to enable SPs, either based on HTTP or CoAP, to easily integrate an authorization layer without the need to implement any complex logic like OAuth. In this paper, the centralized approach is adopted, where the authorization logic is outsourced from the smart and constrained device to a more powerful server called IoT-OAS. The IoT-OAS service, within the EU project CALIPSO [111], has been implemented on a regular web server, based on open source technologies, equipped with HTTP/CoAP proxy capabilities in order to be transparently and easily integrated with all applications. Four significant IoT application scenarios have been illustrated. In addition, the authors strengthen their approach by interesting experimental results obtained during a performance evaluation made by conducting simulations with Cooja targeting Contiki-based Zolertia Z1 nodes. However, the proposed architecture did not consider the end-to-end security integration between Internet and IoT, making the intermediary a single point of security compromising . Furthermore, no mechanisms detailing the issuing of access tokens are described. In this direction, Cipriani and Picone complete and extend the IoT-OAS architecture [110], by proposing a standard-based authorization framework for WoT applications built on IoT- OAS architecture in [112]. The proposed framework provides a set of messages that users can exploit to interact with IoT-OAS in order to manage and request access grants to smart objects. All API calls are authorized by IoT-OAS with OAuth, using the access tokens received upon login. In addition, mechanisms related to issuing of access tokens that can be used to access resources in IoT applications are introduced. An implementation is presented to highlight the simplicity of token issuing. However, even if authors in this paper claim to propose finer granularity in expressing granted access by defining the permission with the following tuple: <res, act, exp> where res is the URI of the resource, act is the REST method to act on the resource, and exp is the expiration time of the grant. The proposed expression is still less granular since it does not take context and smart object ambient environment into consideration. Moreover, authors point out advanced problems that need to be solved when referring to authorization in the WoT. These problems are defined as: (i) Owner-to-Owner authorization (when the object owner authorizes himself to control an object); or (ii) Owner-to-Any authorization (when the object owner authorizes other parties to control an object he owns) and they propose the OAuth 2.0 protocol to address the Owner-to-Owner authorization and the User-Managed Access (UMA) profile [113] of OAuth 2.0 to addresses Owner-to-Any authorization in the web. But, they did not show how this later could be adopted to fit IoT requirement. Finally, both approaches presented in [110] and [112] are bound to the use of OAuth protocol. Therefore, they inherit all the weaknesses of OAuth from an IoT perspective. Those drawbacks will be detailed later on in this paper in Section 4.2.5.

3.3.3. Access control solution based on UMA

[113] describes how the Web Authorization Protocol (OAuth) in combination with User-Managed Access (UMA) can be used for an IoT environment; the paper introduced multiple scenarios with a car, door lock, etc. Those scenarios involve Web, smart phone applications, and IoT devices. UMA is a relatively new access control which is less used in IoT, but offers interesting features, such as user-driven and offline mode. Many IETF efforts [113] are running to adapt UMA to IoT.

A thesis project [114] aims to explore authorization requirements and architecture for user controllable integration of smart things and services. A subset of SWoT [115] projects security requirements has been explored. To realize desired and suitable authorization mechanisms, an extensive study of various security protocols was performed. The UMA protocol which integrates OAuth protocol was determined as adequate mechanism for the envisaged authorization architecture. The specification of the UMA application in SWoT was preceded. In addition, authorization architecture with an UMA framework has been implemented as a prototype for the designed solution. The implementation effort also included the development of software agent's prototypes which could be deployed on smart things or in the cloud, for the purpose of evaluating proposed authorization solutions. More recently, an ongoing work in [116] proposes using the UMA profile to implement access control functionalities in multi-agent IoT-based systems. Authors in this paper provide an overview of related agent-based IoT systems and a brief description of the access control scheme and its corresponding flow applied to multi-agent systems. IoT devices are supposed to contain intelligent agents in combination with other IoT-related functionalities. The UMA Client is considered to be embedded in the device in order to manage requests to use the Message Exchange service. The Authorization Server is considered to be deployed as an independent server accessible by all the other entities in the schema. The protection and access of a resource will be performed as described in the UMA profile within three phases. The first phase consists in protecting the resource, presented in this paper as a queue in the message exchange server modeled as a queue system (i.e. MQTT or AMQP protocols). A communication queue is created in the Message Exchange service and registered within the Authorization Server by the Agent/IoT Device Owner who configures the permissions for users or group of users. (2) Once the queue is protected, the authorization flow starts in the second phase where a Web Client is used by another (or the same) Agent/IoT Device Owner to interact with the Resource Server and the Authorization Server to get the permission required for its agent to access to the registered operation. Finally, a token representing the acquired permission is configured in the Agent/IoT Device by the owner. (3) In the third phase, the properly configured Agent/IoT devices are asked to perform autonomously their tasks (i.e. negotiate for a common goal) through the registered queue. After the process is complete, all the operations will be protected by the access control rules configured in the Authorization Server. Finally, an example scenario is given to illustrate the proposed scheme flow. However, the paper settles for giving a just theoretical description. Neither formal description nor the protocol implementation is provided. The lack of granularity is one of the major drawbacks of OAuth and its profile UMA. To address this potential issue, Vijayaraghavan and Shruti recom-

Table 3
Hardwares specifications.

Hardware specification			[89]	[110]	[107]	[96]	[75]
		Access control model	Usage control	OAUTH	OAUTH	XACML	CAPABAC
Policy Decision Point (PDP)	Localization	Type	Powerful	Powerful	Powerful	Powerful	Powerful
		Platform	Windows 7 professional	*	*	*	Contiki os
		CPU/ micro-controller	Intel core i7 2600 3,4 GH	*	*	*	JN5148 mote RISC processor
		ROM	750 MB	*	*	*	128 KB
		RAM	8 GH	*	*	*	128 KB
Policy Enforcement Point (PEP)	Localization	Type	CLASS C	CLASS B/ C	CLASS C	CLASS B	
		Platform	Windows 7, MQTT broker (Mosquito)	(1) Broker (2) Zolerita MSP430F2617	broker mosquito	Arduino mega 2560 board	
		CPU	*	*	*	16 MHZ	
		ROM	*	52 KB	*	FLASH MEMORY: 256 KB	
		RAM	*	58 KB	*	8 KB	
End device	Localization	Type : Architecture	Constrained Pub/subscribe: behind a broker	PEP =DEVICE	Constrained Pub subscribe	PEP = device	
		Platform	Board linux Debian		Arduino board		
		CPU	ARM 9				
		ROM	256 MB				
Communication protocol between PEP and PDP			HTTP protocol JSON format	*	HTTP	*	PEP =PDP
Communication protocol between PEP and end device			WIFI	COAP /HTTP	MQTT		*

* means: Not available

mend in [117] a Context-Based Data Access Control layer to be integrated with OAuth and UMA. The context awareness layer gets context information from IoT device and pass to inference layer for intelligent implications or computation of values. Access control layer contains a hybrid access control system that combines traditional authorization techniques with sensed context information, to grant access to a legitimate user, device, or application to a requested resource. Authors propose a classification of context-based parameters related to physical factors and others related to human factors. Human factor-related context is structured in three categories: information on user (habit knowledge, emotional state, etc), social environment (co-location, social interaction etc), and activity based (spontaneous activity, engaged tasks, etc.). Similarly, context related to physical environment is arranged into three folders: location (absolute position, relative position, co-location, proximity, etc.), infrastructure (surrounding resources for computation, communication, task performance), and environmental conditions (noise, light, temperature, etc.). Although the suggested model is promising and ambitious, technical details or implementation is not evident and still missing.

3.4. Mechanism layer

We introduced so far the conceptual and formal models proposed in IOT and sketched the architectures. In this paragraph, we outline the low level (hardware and software) functions to enforce policies and define how access requests are evaluated against those policies. We describe in Table 3 the hardware specifications used for the deployment of PDP, PEP, and End device distinctively and the communication protocol between the Policy Enforcement Point (PEP), Policy Decision Point (PDP) and between PEP and end device. We also describe the type of their localization: powerful or constrained, various platforms used, CPU speed and memory size.

Unfortunately, due to the fact that most proposed access control models in the literature have not been developed in practice, yet, an extensive quantitative evaluation is not possible.

4. Analysis & evaluation

After reviewing existing work for each layer in the OM-AM reference model. In this section, firstly, we summarize the strengths and weaknesses highlighted in Section 3 for each refereed access control. Afterward, we elaborate a quantitative and qualitative evaluation based on the fourteen identified Security and Privacy-Preserving objectives. Finally, we present the pros and cons and the usability of the five access control categories defined in our proposed taxonomy from an IoT perspective.

4.1. Strengths and weaknesses of proposed access control solution in IoT

The issues and drawbacks with existing solutions, extensively highlighted in Section 3 are summarized in Table 4:

4.2. Quantitative and qualitative evaluation

In this section, we evaluate in both qualitative and quantitative way the literature advances towards access control in IoT and their versatility for preserving security and privacy by referring to the above described fourteen objectives. The fourteen S&PP objectives defined in Section 3.1.2 will be the quality criteria of our analysis and comments.

Table 4
Strengths and weaknesses of refereed access control solutions proposed in the literature.

References	Pros	Cons	Implementation
[50]	The mapping of device and web service offers great interoperability and heterogeneity	Old approach more oriented web than IoT	No
	Add context as constraint to take access control decision	The role of smart thing is neglected in taking access control decision	
		Critical scalability: (mapping of one device to many web services)	
		Device to device communication is not considered	
[53]	Integrating Social Network Services (SNS) with access control model offers great usability and allows Resource owners to define personalized access policies in a costumer way	Not context aware	Yes
		Require implicit trust of (SNS) providers.	
		Device to device communication is not considered.	
[54]	Careful mapping between RBAC entities and WoT component	Centralized approach (all access control logic is externalized to ADF entity)	No
		End device plays limited in making access control decision	
		No mechanism is proposed to extend RBAC to fit a distributed and dynamic environment such as the WoT	
[56]	Combine authentication and authorization	Authorization process is slightly described	No
		No specification of access control policy	
[59]	Fine grained access control for end devices in the perception layer of IoT	Complex management of access control in constrained devices	No
[62]	Dynamic and granular access control due to the mutability of UCON attribute	Only conceptual model	No
	Strong expressiveness of usage control compared to traditional access control	Centralized	
[69]	Device to device communication is considered.	Not context aware	Yes
	Delegation is supported.	specification of CAC propagation and revocation is left unaddressed	
	Supports heterogeneous technologies (WiMAX, WIFI, Bluetooth, 4G)	Missing lightweight version of CAC supported by constrained device.	
[71].	Introduce context constraint in ICAP [secure]	Requires prior knowledge and trust relationship between two network domains in federated IoT	NO
	Delegation method in federated IoT		
	Distributed		
	Device to device communication is considered		
[72]	Support of delegation and revocation mechanism	Smartness in device side is neglected.	No
		Deals with IoT as usual computing platform	
[75]	distributed	Lack of granularity and context awareness	Yes
	Use of lightweight protocols		
	scalability		
[83] and [84]	Projection of OrBAC notion in IoT paradigm	Too heavy and complex to be supported by constrained devices	No
	Support of granular and context aware access control policy		
[88]	Scalable	centralized	Yes
	flexible	lack of integration with an access control model	
[79]	Multidimensional approach	Lack of fully distributed approach	Yes
	Flexible and lightweight mechanisms are used	A well-defined interoperable negotiation language is missing	
	The proposed trust model is integrated with DCapBAC access control model		
[89]	Powerful tool to express granular access control policies	Complex to design and maintain	yes
[95]	Fine-grained access control policy is supported	Device to device communication is not considered	Yes
	IoT device heterogeneity is considered	Constrained nature of IoT devices is neglected	
[96]	Takes IoT device local parameter in access control decision	Too heavy to be embedded in constrained IOT devices	Yes
[106]	User-centric solution	Not scalable	YES
	Very usable due to the use of popular SNS such as Facebook, Twitter etc	Device to device communication is not considered	
		Not context-aware	
[107]	First to implement OAuth over MQTT protocol	Usage control and simplicity of key issuing are missing	Yes
	User-directed access control		
[108]	First to add support for IoT specific protocol such as MQTT to API management system	Centralized	Yes
		Not user-driven	
[110]/ [112].	Both HTTP and COAP based SP are enabled to integrate authorization layer without the need to implement any access control logic	Centralized	yes
		Not context-aware	
[116]	Use of specific IoT protocol such as MQTT with UMA	Neither formal description nor implementation is provided	No
	Projection of UMA components in IoT context		
[117]	Context aware	Only theoretical recommendations are provided	No

Based on the described legend below this evaluation is highlighted as follow:

Legend: VH= Very high => 5, H= high => 4, M= Medium => 3, L= Low => 2, VL= Very low => 1, No= Null => 0

Each quality criteria is assigned a value ranging from 0 to 5, where 0 signifies not defined, 1 signifies a very low quality sufficiency, 2 signifies a low quality sufficiency, 3 signifies a medium quality sufficiency, 4 signifies a high quality sufficiency while 5 signifies a very high quality sufficiency. These values are then used to indicate the sufficiency of each referred access control solutions for each S&PP objective. All refereed solutions have been surveyed qualitatively, by comprehensively analyzing all the specification documents as well as any related research papers, and by mapping them to our requirements. The assignment of values in the 0 to 5 range within each quality criteria for each referred access control solutions is performed as follow:

- Context awareness
  We notice that except the work presented by Vijayaraghavan [117], all solutions based on UMA and OAuth protocols do not take context into consideration in access control decision. Actually, authors in [117] propose a Context-Based Data Access Control layer to be integrated with OAuth and UMA. A comprehensive classification of context-based parameters related to physical factors and others related to human factors ranging from information related to user (habit knowledge, emotional state, etc), social environment (colocation, social interaction etc), and activity based (spontaneous activity, engaged tasks, etc) to information related to physical environment such as location (absolute position, relative position, colocation, proximity, etc), infrastructure (surrounding resources for computation, communication, task performance), and environmental conditions (noise, light, temperature, etc). Due to this rich classification, we rank this solution regarding context awareness criteria as very high. In the second range, comes two proposed solutions that are: the SmartOrBAC model [83] and [84] that enhances the context notion in OrbBAC and CCAAC [71] where an additional field called Contexts (C), which contains context information related to the capability, is added in the extCAP. Both models use the same definition and expression of context notion where context is considered as set of contexts (CSet) with different types (CType). The type of context can be a concrete property such as time or location, but also security-related context such as authentication and trust level. In order to apply the context in the access control decision, each of the context types has to be evaluated with a certain constraint (CConst). The adopted definition qualified both works regarding context- awareness criteria as high level. It is worth to note that CCAAC[71] is the only solution, to the best of our knowledge, based on capability model that takes context into consideration. Other solutions citeGusmeroli2013, [69] and [75] do not. By definition, the RBAC model does not consider contextual information in access control decision making. It is the same case for the solutions based on pure RBAC such as [53] and [54] except [50] that extends RBAC by the introduction of context constraint collected from the environment of the physical object. For this reason, we classify this solution at a medium level. In the same level, we gather attribute- based access control solutions such as [59,62,95] due to the fact that attribute may correspond to contextual information except for the solution presented in [96] qualified in a high level of context awareness. Actually, authors in [96] take explicitly devices local parameters before the enforcement of access control decision locally enabled via XACML obligation. Finally, we consider solutions based on trust model such as [88] and [79] in a low level of context awareness because the context is not explicitly considered.
- Interoperability
  The web service technology is known to provide great interoperability between heterogeneous devices. For this reason, we classify all the solutions that adopt the web of thing approach (based on web service) as high-quality sufficiency in term of interoperability. Those solutions are: [50,53,54,56] and [106]. Other solutions have a very low interoperability sufficiency since this criterion is not tackled in a focused way.
- Heterogeneity
  We consider that the solution proposed by Kim et al. in [95] has a very high heterogeneity sufficiency since it uses an extensible (Open Services Gateway initiative) OSGi-based architecture for highly heterogeneous smart home systems to enable dynamic integration of devices and services. In the second range comes the web of thing based solution [50,53,54,56] and [106] that have high heterogeneity sufficiency level due to the use of web service technology that provides great interoperability between heterogeneous devices.
  Capability based solution [69,71,72,75] are classified in the third range with medium heterogeneity sufficiency level. Actually, by design, the scheme of capability based access control solution works efficiently for heterogeneous devices Other solutions have a very low heterogeneity sufficiency since this criteria is not tackled in focused way.
- Scalability and flexibility Token based approaches that include both capability based model [69,71,72,75], OAuth based protocol: [106–108,110] and [112] and UMA based protocol [116] and [117] are characterized by great scalability and flexibility. In addition, the FTBAC scheme [88]is simulated and results show that it can be used to calculate fuzzy trust values for any number of devices which makes it more suitable for scalable IoT. For those aforementioned reasons, we classify those solutions with high scalability sufficiency. However web of thing based approach solutions [50,53,54,56] and [106] present a medium level of scalability and flexibility because the mapping between web services and IoT devices may rise scalability issue. Solutions based on attribute-based access control [59,62,95] have a low scalability level.
- Usability and user-driven
  The integration of network service (SNS) puts forward both solutions [106] and [50] to be characterized by a very high level of usability and user-driven sufficiency feature. Furthermore, UMA and [89] are by design user-driven access control protocols. For this reason, solutions based on UMA, such as [116] and [117], are with a high level of user-driven sufficiency. However, usability of those solutions is not clearly handled. RBAC and Attribute based access control solutions such as [50,53,54,56,59], [62,95,96] are classified in the third range with medium low usability and user driven sufficiency level. Actually, those models are not conceived with user driven feature in mind. Other solutions have a very low user driven and usability sufficiency since these criteria are not tackled in a focused way. Although, the proposition in [89] is a user-centric solution. The generation of many different profiles and different versions makes the framework extremely complex to handle and maintain. Actually, the complexity to use the framework is highly bounded to the complexity of the environment where the user is active. Unless an automation tool is conceived to automate the choices for the user, its level of usability sufficiency is very low.
- granularity
  In one hand, [89] is considered to be a powerful tool to express granular access control policies. It is a collection of

meta-models that describe Data, Time, Identity, Role, Structure, Behavior, Trust, Rule, and Risk. In another hand, the solution proposed in [62] based on UCON model enables the expression of granular access control policies due to the high level of expressiveness and dynamicity of UCON attribute. For those reasons, we rank those solutions regarding granularity criteria in a very high level of sufficiency. In the second range, comes the attribute based access control models [96] and SmartOrBAC [83] and [84] based on OrBAC model. This range of solutions that supports fine-grained access control policies are classified with a high level of granularity sufficiency. In the same range, we classify CCAAC [71]. Actually, we notice that CCAAC could be considered as an exception in access control solution based on capability model category due to the fact that it enables the expression of relatively granular access control policies. In fact, CCAAC includes an additional field C that refers to Context information in capability scheme. Furthermore, CCAAC claimed to be a special case of UCON where capabilities are modeled as subjects and objects attributes and can be propagated through mutable attributes.

In the third range, we classify both [79] and [88] in a medium granularity sufficiency level. Actually, [79] takes into account four dimensions: reputation, quality of service, social relationship between IoT devices, as well as security aspects as parameters to express access control policies and [88] supports 27 possible rules derived from linguistic terms such as (Good, Very Bad, and Below Average) used to express different access control policies. In the fourth range, we classify capability based access control models [69,72] and [75] in a low level of granularity sufficiency since those solutions lack granularity and context-awareness. Finally, the OAuth and UMA-based access control solutions [106–108,110,112] and [116] are classified in a very low level of granularity since this feature is insufficiently satisfied.

- Lightweight

  In one hand, [75] uses lightweight technologies such as JavaScript Object Notation (JSON) as representation format for the token, the emerging communication protocols such as CoAP [77] and 6LoWPAN [78], as well as a set of cryptographic optimizations for ECC . In the other hand, [107] implements OAuth2 with MQTT and Arduino board and IACAC [69] which is compatible with the lightweight, mobile, distributed, and computationally limited nature of IoT devices plus existing access technologies like Bluetooth, 4G, WiMax, and Wi-Fi. It uses public key cryptography approach based on an elliptic curve on finite fields ECCDH that has advantages of small key size and low computation overhead. Those both described solutions are classified at a very high level of lightness.

  [89] has been implemented as an extension to the open source broker Mosquitto in [91], and [110], [112] proposed an architecture designated for services providers (SPs) , either based on HTTP or CoAP protocols. Both solutions use IoT particular lightweight protocols: MQTT and COAP, putting forwards those two solutions to be classified in a high level of lightweight sufficiency.

  Seitzs solution [96] faces the verbosity feature of XACML by proposing compact representation in JSON for assertion format. Nonetheless, the solution is still too heavy to be embedded on device side. That is why we classify this solution in a medium level of lightweight sufficiency.

  Capability based access control models [69,71,72] and [75], OAuth and UMA [106–108,110]/[112,116] and [117] are considered in a low level of lightweight sufficiency. While RBAC and attribute-based access control solutions present a very low level of lightness.

- Distribution

  In [75] and [96], a great part of the decision making process for granting access is externalized (externalized PDP). However, the decision of access control is enforced locally by the object (local PEP) taking its local parameters into consideration. Local decisions are enabled via XACML obligation. Based on those aforementioned features, we classify those two solutions with a high level of distribution efficiency. [69] and [71] have a medium level of distribution sufficiency for the following reasons: (1) Devices are connected with each other through the use of an access point. (2) Any device that wants to communicate with another device is able to initiate the communication by sending the request to a specific device. (3) Each established communication is verified by its capability access. [116] is included in the same level with [69] and [71]. Actually, UMA Client is considered to be embedded in device side in order to manage access requests while the Authorization Server is considered to be deployed as an independent server. The OAuth-based access control solutions [106–108,110] /[112] present a very low level of distribution sufficiency since all authorization logic have to be externalized to a powerful entity as demonstrated by [110]. The centralized approach is adopted in the rest of other solutions cited in this survey where the authorization logic is outsourced from the constrained device to a more powerful entity.

- Real-time

  Only two solutions from the studied literature in this survey paper tackle real-time issue in an explicit way. Those two solutions are the UCON model presented in [62] and [89]. In one hand, UCON is more suitable to meet the dynamic nature of IoT. This particularity resides in the concept of continuity of decision and mutability of attributes introduced by UCON model. In the other hand, the specification of authorization and obligation policy rules is done in [89] using an event-based Rule model containing Rule Templates. Events represent actual or tentative events which mean respectively activities in the IoT system that already took place or are about to take place but have not yet started. The aforementioned features make those two solutions characterized by a very high real-time sufficiency level. CCAAC [71] claims to be a special case of UCON where capabilities are modeled as subjects and objects attributes and can be propagated through mutable attributes. For this reason, we consider this solution in a high level of real-time sufficiency. However, all other solutions did not consider real-time parameter into consideration in their papers.

- Delegation and revocation

  Delegation and revocation are explicitly addressed in [72] and [71]. Researchers presented an access delegation method with security considerations based on Capability-based Context-Aware Access Control (CCAAC) model intended for federated IoT networks. However, other solutions consider neither delegation nor revocation features directly.

- Offline mode

  Except the solutions [116,117]based on UMA protocol, no other solution supports offline mode straightforwardly.

We summarize the previous evaluation of the literature based on the P&SP objectives in Table 5.

Once all sufficiency values have been determined, the final generic quality value for each access control category can be calculated as shown in the graph depicted in Fig. 4 that highlights in a very representative way how each category meets each requirement.

4.2.1. Evaluation of access control solution based on RBAC model

We notice that solutions based on RBAC model have the following issues:**(1) Interoperability**: the difficulty to approve a real

Table 5
An evaluation of related work based on IoT S&PP objectives.

Access control model	Citation	Scalability	Usability	Flexibility	Interoperability	Context awareness	Distribution	Real time	Heterogeneity	Lightweight	User-driven	Granularity	Revocation	Delegation	Offline mode
RBAC	[50]	M	M	M	VH	M	NO	VL	H	VL	M	M	NO	L	VL
	[56]	M	VH	M	VH	VL	NO	VL	H	VL	VH	M	NO	NO	VL
	[54]	M	M	M	VH	VL	NO	VL	H	VL	M	M	NO	NO	VL
	[53]	VL	M	VL	VL	VL	NO	VL	VL	VL	M	M	NO	NO	VL
ABAC	[59]	M	L	M	M	H	NO	VL	VL	VL	M	M	NO	NO	VL
UCON	[62]	L	M	L	L	H	NO	VH	VL	NO	M	VH	NO	NO	VL
CAPBAC	[71]	H	M	H	L	H	M	H	M	L	M	H	L	VH	M
	[72]	H	M	H	L	VL	M	VL	M	L	M	L	L	M	VL
	[69]	H	M	H	L	VL	H	VL	M	L	M	L	VH	VH	VL
	[75]	H	M	H	L	VL	H	VL	M	H	M	M	H	H	VL
XACML	[95]	L	M	L	L	M	H	VL	M	VL	M	M	VL	VL	VL
	[96]	L	M	L	L	M	H	VL	M	M	M	M	NO	NO	VL
OAUTH	[106]	H	VH	H	VH	VL	VL	VL	VL	L	VH	VL	VL	VL	VL
	[107]	H	M	H	L	VL	VL	VL	VL	L	H	VL	VL	VL	VL
	[108]														
	[110] [112]	H	H	H	L	VL	M	VL	VL	L	VH	VL	VL	VL	VL
UMA	[116]	H	M	H	L	VL	VL	VL	NO	VL	H	L	VL	VL	VH
	[117]	H	M	H	L	VH	VH	VH	NO	VL	H	L	VL	H	VH
Others	[89]	VL	L	VL	L	VH	VH	VH	NO	VH	L	L	VH	VH	VL
	[79]	VL	L	VL	L	L	L	L	H	VL	L	H	L	M	VL
	[88]	M	L	H	L	L	L	L	NO	VL	L	L	L	M	VL

Table 6
RBAC pros and cons from an IoT perspective.

Access control solutions based on RBAC model	Pros	Cons
	Least privilege	Interoperability
	Separation of administration function	Critical scalability
	Support constraint	Role explosion
		Critical granularity
		Limited dynamicity
		Not User driven

consensus regarding the meaning of role to be shared with different applications, platforms, domains and enterprises. **(2)Role explosion**: The role explosion issue justifies the critical dynamicity aspect of RBAC. Actually, RBAC defines access permissions in a static and fixed manner without taking the context of the access into consideration. As a result, a pure RBAC solution may be inappropriate for defining fine-grained access permissions based on context, and dynamics of IoT environment. **(3) Critical scalability:** policies cannot evolve easily. In fact, the creation of new roles can lead to rebuilding the entire model. **(4) Nonsupport of delegation**: a subject cannot grant access rights to another subject, as well as grant the right to further delegate all or part of the granted rights. Due those issues, basic RBAC model is not really a suitable solution to perform authorization functions in IoT domain applications requiring high level of interoperability/scalability, such as smart grids and smart cities. Even for domain applications such as wearable, entertainment and home, where the management of Roles may be less complicated than in other domain applications, the issue of role explosion prevents RBAC from encapsulating expressive, contextual and dynamic access control policies. Indeed, IoT needs fine-grained and self-configuring access control mechanisms that emulate the dynamicity present in everyday life (e.g. Grant a neighbor access to home appliances in case of emergency). The pros and cons of RBAC based access control solutions from an IoT perspective are summarized in Table 6.

4.2.2. Evaluation of access control solutions based on ABAC model

We can conclude that ABAC have more advantages that make it more appropriate for utilization in large-scale distributed systems such as SmartGrids applications in IoT. These advantages are: (1) Interoperability: ABAC model eases interoperability especially in collaborative environments, since it allows unknown user to access resources as long as their attributes meet certain criteria. (2) Fine-grained access control: Unlike RBAC, ABAC model is more expressive since it defines access right based on attributes. These attributes could be any relevant security-characteristics that describe all entities including resource, subject and environment. This makes ABAC more relevant to provide fine-grained access control. Despite all the above-mentioned advantages, there are cons and challenges to the adoption of ABAC in IoT. Indeed, the use of attributes for authorization comes with several constraints: **(1) Complexity:** Semantic interpretation of attributes, their trustworthiness and the definition of syntax for expressing attribute-based authorization requests and responses are all main reasons to make ABAC more complex. Besides, the complexity of XACML often pushes users to avoid its use and to use more traditional approaches instead. This is the case of the medical application discussed in [118]. This complexity also hampers its utilization in everyday scenarios, for example, in application domains belonging to category wearable entertainment IoT applications. However, it could be a potential candidate to model policies in application requiring high interoperability and sophisticated level of expressiveness. **(2) Not User-driven:** Although XACML and ABAC are considered as complete and accurate policy description methods, the structure of an XACML

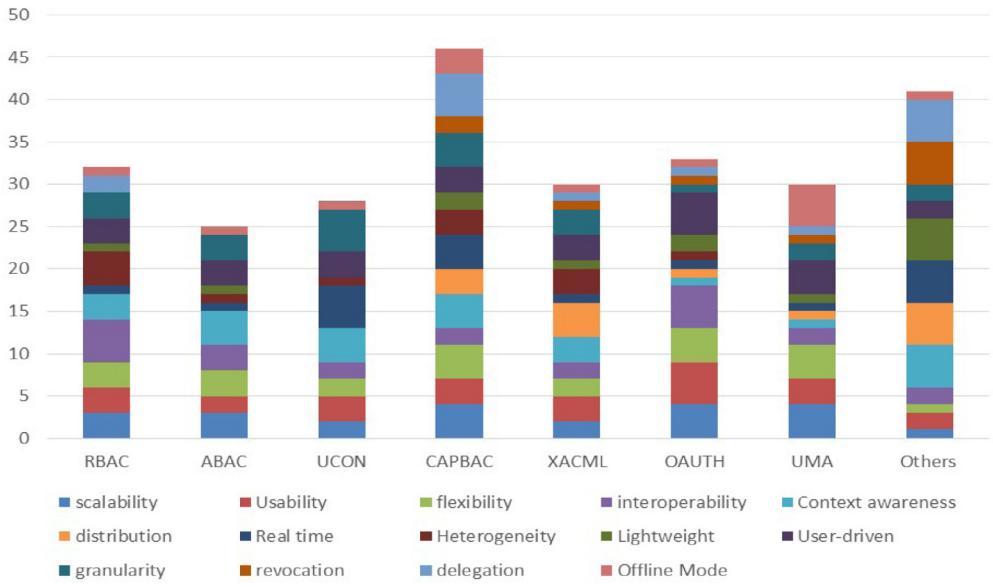


Fig. 4. A quantitative evaluation of access control solutions proposed in the literature in IOT.

Table 7
ABAC and XACML pros and cons from an IoT perspective.

ABAC	pros	Cons
	Fine grained	Complexity
	More scalable	Not user-driven
	More flexible	
	More interoperable	
	Support of delegation	

Table 8
UCON pros and cons from an IoT perspective.

UCON	PROS	CONS
	High dynamicity	No functionality for administration
	Mutability	No delegation
	Fine-grained	Complexity
	Flexible	Not user-driven
	Scalable	

policy is complex. Indeed, user is obliged to understand XACML very well and write down the verbose policy skillfully. This makes XACML difficult to master and to use. This type of privacy management does not support interactions with the user in a native way. A user-driven privacy manager is needed in order to involve the user in the policy definition process. The pros and cons of ABAC model/ XACML standard from an IoT perspective are summarized in Table 7.

4.2.3. Evaluation of access control solution based on UCON model

We notice that solutions based on UCON model have high level of granularity and context awareness thanks to the high expressiveness of UCON ABAC model, but have low level of distribution, usability and lightness. Indeed, the first solution is based on an extended architecture of SOA and the access control logic is expected to run on powerful devices. However, the second solution of Neisse is based on extended model of UCON which is very expressive. In addition, it has been enforced at the Message Queuing telemetry Transport (MQTT) [92] layer but on powerful devices. Hence, its feasibility in constrained devices has not been demonstrated. The pros and cons of UCON model from an IoT perspective are summarized in Table 8.

Table 9
CapBAC pros and cons from an IoT perspective.

CapBAC	Pros	Cons
	Flexibility	Coarse-grained
	Distributed	Do not take context into consideration
	Simplicity	Problem of propagation
	User-driven	
	Support Revocation	
	Support Delegation	
	Usability	

4.2.4. Evaluation of access control solutions based on CapBAC model

CapBAC presents some great advantages from an IoT perspective. It shows great scalability, flexibility and usability. In category: wearable, entertainment and home where applications are more tied to everyday life scenarios and characterized by spontaneous and unpredictable relationship, Resource owner could consider the usage of time-limited capability tokens and restrictive delegation usage. In category: enterprise and government where interactions pattern are qualified as medium to long such in B2B for example, Capability tokens with extended validity periods could fit in an efficient way this kind of use cases. Furthermore, it supports delegation and revocation. The pros and cons of CapBAC model from an IoT perspective are summarized in Table 9.

4.2.5. Evaluation of access control solution based on OAUTH protocol

OAuth protocol and framework is characterized by its high scalability, flexibility, simplicity, but it lacks fine granularity and offline mode features[110]. has demonstrated the impossibility to run all OAUTH logic in a constrained device due to its heavy communication and processing overheads. However, the IETF is making continuous efforts to adapt OAUTH protocol with lightweight protocols, such as COAP and DTLS, in order to make OAuth fit IoT requirements [77,119–121]. Its main pros are: (1) the introduction of human users role incarnate by resource owner. (2) Relative simplicity and design that relies on specific Web technologies which are considered as best practices in design of web based solutions (such as RESTFUL design, JSON encoding format, adoption of TLS for transport layer security, etc.). (3) High scalability improved by its success to manage access rights of the unbounded number of users in social networks. (4) The revocation of

delegated permissions: Thanks to the approach of refresh token and expiration of access after some time, the client is enforced to re-authenticate and re-verify its access. The user is also enabled to revoke the granted access. (3) Identity interoperability: OAuth and other OAuth-based protocols such as User-Managed Access (UMA) [122] and OpenID Connect 1.0 [57] will enable, in IoT, identity interoperability. Indeed, the unbounded numbers of connected devices are created by different manufacturers and belong to different identity providers. For example, if a user has a connected car VOLVO XC90, a Google smart watch, a Fitbit monitoring calories, and LIFX light bulb controllable with his smartphone, he will be obliged to create and manage unique credentials (username, password) for each device corresponding to its provider. Thus, the use of OAuth will eliminate the need for the user to create an account for every service provider by enabling these latter to accept, trust and use an identity created and managed by another, whether that be another IoT service provider like Google or a social network like Facebook acting as trust hub. But this will concentrate identity in such a hub and, in the long term, will prevent users from freely controlling their data. The main cons and challenges to the adoption of OAuth to IoT are: (1) Difficulty to achieve a secure implementation: There is always a tradeoff between security and usability. In fact an empirical analysis of existing implementations of the protocol, conducted by [123], showed the difficulties to achieve a secure and reliable implementation given its open specification and the quantity of security factors to take into account. (2) OAuth is tied to a number of assumptions adopted during its design: as a result, OAuth does not cover all security requirements for systems not complying with those assumptions. Unfortunately, OAuth was not designed with IoT specific requirements in mind, and will not consequently cover all its security needs. For example, OAuth assumes that the services in need to be protected are implemented and managed by the same business entity. Moreover, OAuth supposes that the type of resources to be secured is known at design time, which is not always the case in IoT scenarios. (3) Coarse-grained: scopes, which determine the privileges and the level of access that should be granted to a Client application requesting access to the Resource Owners resources, are determined at design time, and are typically coarse-grained. (4) Not user-driven: Defining authorization scope by the serviced provider at design time induces a lack of security transparency from the Resource Owners perspective and prevents him to define his own access control policies over his resources hosted in a SPs side. (5) Disclose privacy: OAuth entrusts service providers the responsibility to define the permissions the consumer can request. However, most providers solely define an extent set of access rights, such as complete access to data or read-only, which is contradictory to privacy preserving objectives [124].(6) Heavy implementation especially on Service Provider SPs side: implementing OAuth on the SPs side is a complex, time-consuming, and computationally intensive task. In addition, it implies the registration of both users and client applications, and the permissions that User grants to consumer applications. This process extremely hinders the implementation of OAuth logics on constrained devices. we summarized the pros and cons of OAuth protocol from an IoT perspective in Table 10.

Table 10
OAuth pros and cons from an IoT perspective.

OAuth	Pros	Cons
	Flexibility	Coarse grained
	Lightweight	Prevent user from freely controlling his data
	Scalability	Lack of robust Security
	Widely adopted	Lack of secure implementation
	Simplicity	Lack of implementation interoperability
	Revocation	Heavy implementation in SP side
	Introduction of human users role incarnate by resource owner.	Do not support least privilege principle
	Identity interoperability	Concentrate identity on central hub
	Support runtime creation of an authorization context	Not user-driven
		tied to a number of assumptions adopted during its design

Table 11
UMA pros and cons from an IoT perspective.

UMA	PROS	CONS
	User-driven	New (has not yet a stable version)
	Support claim-based access control	centralized
	Pre-arrange rules	
	Off line mode	
	Externalization of authorization	
	Support claim-based policies	

4.2.6. Evaluation of access control solutions based on UMA

UMA can be a promising solution for IoT. More relevant pros of UMA are: Pre-arranged rules: Unlike OAuth, which is conceived for synchronous permission, UMA allows asynchronous permission based on pre-arranged rules. Offline mode: UMA does not require the grantor access to be online at the time of access request since it handles granting of entitlements (through scopes), asynchronously. User-driven: UMA brings a novel approach by including user as a core part of its model. The proposal relies on the user to assign access rights to resources that may be hosted at various resource servers. In fact, the user has the responsibility to define and configure his own policies required to make access control decisions. UMA uses a centralized authorization server that facilitates data sharing in a selective way and based on users own instructions. Support for claim-based access control in order to enable access decision to be dynamic and to enable the user to impose contract terms that control access rights before the authorization is granted. UMA introduces the notion of claim which is a set of identity attributes of a requesting party that an AM may need to gather in order to satisfy some properties, imposed by the user, before access to a protected resource. UMA is based on OAuth and inherits consequently its drawbacks regarding interoperability and secure implementation. The pros and cons of UMA protocol from an IoT perspective are summarized in Table 11.

5. Discussion and open issues : authorization and access control challenges in IoT

From the previous state of the art, the major emerging challenges related to access control can be deduced from two fundamental questions: (1) Will existing access control technologies and standards still be used in IoT or will they just need to be adapted to the constrained environment imposed by IoT? Do we need to come up with new access control mechanisms with IoT specific requirements in mind? (2) Is it more effective to exploit a centralized, distributed or an hybrid approach in order to manage access control in scalable IoT architecture?

5.1. Challenge 1: adapt existing access control mechanisms versus conceive new ones with IoT specific requirements in mind

The integration of physical objects in the internet infrastructure requires the application of lightweight security mechanisms to be used even in constrained environments. However, current security standards and access control solutions were not designed with such aspects in mind. They are not able to meet the needs

of these incipient ecosystems regarding scalability, interoperability, lightness and end-to-end security. Consequently, a deep revision and adaptation of those mechanisms needs to be considered. These challenges have attracted more and more attention from research community and recently several efforts are starting to emerge in this direction. Actually, there are two main approaches that have been introduced in the literature. The first one consists in adapting existing solutions to meet IoT requirements and needs. The second approach consists in rebooting and rethinking internet and conceiving from scratch specific technologies including access control solutions with IoT characteristics in mind. In this section, both approaches are discussed.

- **Adaptability approach**: Recently, numerous efforts have emerged in this direction, and several IETF Working Groups are focused on the adaptation of existing Internet protocols that have been developed in (i) the building blocks of the Internet of Things (e.g. sensor networks, ad-hoc networks) and (ii) other paradigms closely related to the Internet of Things (e.g. ambient intelligence, pervasive computing). In fact, some security mechanisms, such as key Management, have been successfully adapted to certain IoT scenarios [125]. In this approach, the answer to IOT security is to not re-invent the access management experience. The patterns and protocols, which are now available to protect Web resources, should be carried over to IOT. Actually, adapting existing techniques to resource constrained devices, rather than developing new approaches towards the wider IoT requirements, will save time and lets developers focus on service logic rather than on security and authorization issues.
- The reboot approach: it consists in designing and developing new technologies specific to IoT requirements and needs based on the following aspects: (1) Typical security and access control standards are built around a single logical server and multiple clients. As a consequence, access control is often done within the server side application, once the client has been authenticated. IoT reverses this paradigm by having many devices serving as servers and possibly many clients, taking part in the same application. More importantly, servers are significantly resource-constrained, which results in the minimization of the server side functionality. Subsequently, access control becomes a distributed problem, especially when taking into account the recent efforts of decoupling the sensor network infrastructure from applications [126,127]. (2) IoT has new specific Business model and characteristics and absolutely differs from usual computing platforms. Therefore, adopting existing access control solutions will only lead to complex, expensive and less adoptable solutions. (3) After Snowden scandal, trust in the internet is over. Building IoT solutions with centralized and collaborative system composed of trusted stockholders is now something of a fantasy. Most access control solutions today enable centralized authorities (e.g. governments or service providers such as Facebook or Google for example) to gain access and control devices by gathering and analyzing user data.
- **Summary**: In the adaptability approach, the solutions are mostly web based. As a result, their adaptation requires implicitly the adoption of the web-of-things approach. The question of “Web” vs. “IoT” can in some cases be considered a continuum and unfenced debate. Significant effort has been made on securing existing Internet standard authentication and authorization protocols such as TLS, Kerberos [128], OAuth, and traditional access control models among others. Although, expanding the feasibility of these solutions to constrained environment such IoT would save huge effort. These protocols were substantially not designed with constrained environments in mind. As a result, adjusting an existing solution could arise a far from optimal one. Commonly used Internet protocols cannot in every case be applied to constrained environments. In some cases, adapting and profiling is required. In other cases, it is advantageous to define new protocols which were designed with the special characteristics of constrained environments in mind.

5.2. Challenge 2: centralized versus distributed

- Centralized approach: This approach consists in relieving smart device from the burden of handling a vast amount of access control-related information by outsourcing these functionalities to a back-end server or gateway which is responsible for security tasks. This approach presents many advantages: **(1) Possibility to reuse existing technologies:** Indeed, since the back-end or the gateway which is responsible for access control is not a constrained device, it is possible to reuse traditional and current access control models, security standard technologies and protocols. But in this case, objects are treated as dumb devices, which is in contradiction with the essence of IoT that consists in bringing smartness to the edge of the network. **(2) Ease to manage access control policies:** authentication and access control policies are easier to manage in centralized IoT architectures, all access control policies are stored and managed within a single central entity. Therefore, data providers do not need to implement any kind of access control logic. They will send all their data to those whom they trust. As flip side of this approach, both data providers and information consumers must fully trust the central entity. However, several drawbacks arise with the real deployment of the centralized approach. They are summarized as follows: **(1) End to end security:** the inclusion of a central entity prevents end-to-end security to be achieved. **(2) Single point of failure**: due to the fact that a single entity stores and manages all the data from a set of devices, any vulnerability might compromise a vast amount of sensitive information and even cause disastrous obstruction to the whole system. **(3) User is not involved in access control over his own data**: When access control logic is located in the cloud or in a central entity, they have a full control over the hosted resources. As a result, user’s control can be weakened. **(4) Expensive management**: managing all IoT devices in a centralized way would be too expensive in the long term. IoT devices are envisioned as low-cost, low-maintenance devices that should run for years and even decades. **(5) Trust foreign entities:** Delegating the authorization logic to an external service requires a strong trust relationship between the delegated entity and the device. Moreover, all communications between them must be secured and mutually authenticated, so that the delegated entity security level is at least as high as if the authorization logic were implemented internally.
- **Distributed approach**: The concept of a distributed IoT is a promising approach to release IoT [8,129,130]. As devices increase their computational capacity, there are more opportunities to bring intelligence on the devices themselves. The development of autonomous, decentralized architectures and the location of intelligence mainly security and access control logics at the very edge of the networks are issues that need to be addressed. Actually, this approach presents the following advantages: **(1) Data management and privacy**: Distributed approach brings noteworthy impact in this domain. Actually, with the edge intelligence principle, users have more control over the granularity of the data they produce as they are more enabled to define their own access control policies. **(2) Cost**: it is less expensive than providing a cloud back end for each connected smart object, especially those that might need a connection for a decade. **(3)User involvement in security mechanisms configuration**: as more as the intelligence is located

Table 12
Access control challenges in IoT environment.

Challenges	Approaches	
	Adaptability approach	Reboot approach
Challenge 1: Using existing access Control mechanism vs Come up with new ones	Pros: (1) Exploit already existing and long experience. (2) Saving time Cons: (1) Complex solutions. (2) Do not fit with IoT new business model. (3) Existing solutions meet the scalability of IoT Centralized approach	Pros: (1) Fit the new IoT business model. (2) Comply with the principle of privacy by design. (3) Built with IoT requirements in mind Cons: (1) Need time to be built. (2) Need trust to be investigated, developed and adopted Distributed approach
Challenge 2: Centralized access control management vs Distributed access control management	Pros: (1)Possibility to reuse existing mechanism (2)Ease to manage access control policies Cons: (1) End to end security is dropped (2)Single point of failure (3) Not user-driven (4)Expensive management (5)Trust foreign entities	Pros: (1) Ensure privacy (2) Less expensive in cost (3) Offline mode (4) Support trust Cons: (1) Complex security mechanisms (2) Fine-grained access control logic not supported by constrained devices (3) Difficulty to manage and update access control policies embedded in device side

in the endpoints of the network. User-centric networks are emerging increasingly in IoT. Subsequently, end-users are getting more empowered to create and manage their own access control policies. Thus, the user-driven feature is a must for an access control model to fit IoT needs. However, as side effect of this approach, end-user are not expected to be experts to use security mechanisms. A simple mistake or a misconfiguration can lead to huge breaches in their privacy. For this reason, access control, mainly within the decentralized approach, have to be enough usable for ordinary people. Otherwise people cannot individually protect their IoT devices in their house and would be obliged, in some cases, to remedy to centralized access control management. **(4) Offline mode**: in on-site intelligence approach, the core functionality continues even if the connection is lost. **(5) Support of trust:**Trust could be supported in a better way with the decentralized approach than the centralized one because policies can be defined at the edge of the networks and there will be no need to introduce any central entity.

Nonetheless, the decentralized approach presents the following drawbacks: **(1) Complex security mechanism**: a distributed IoT needs to implement various distributed mechanisms to manage and enforce these policies, which is not evident. **(2) Access control logic is not supported by constrained devices**: implementing an authorization mechanism on the devices side is more complicated. It requires intensive and computational capabilities which are not available, especially in devices like sensors, actuators or RFID tags etc. **(3) Difficulties to manage and update access control policies:** if the access control logics resides in the device locally, it would be highly onerous if not impossible, to remotely and dynamically update them, especially when these devices are placed in unreachable or hardly attended location (e.g. Fastprk1 by World sensing, a smart parking systems, where devices are embedded directly in the asphalt).

By reviewing the advanced analysis, we can conclude that no approach is better than the other. All of them have various advantages and disadvantages. We can conclude that both approaches (centralized and distributed) can complement each other.

We summarize the pros and cons of both approaches in both challenges in Table 12:

6. Innovation trends and research future directions in IoT

The nature and the complexity of IoT environment is opening interesting discussions about how the authorization and access control mechanisms can be applied to this context. Based on the above literature review of the current access control models, and the latest innovations in IoT in general and access control in particular, key future research directions are identified as follows:

- **Smartness shifts from the center to the edge of the network: device-driven democracy**: IoT needs a new access control framework suitable for the distributed nature of IoT, where power and intelligence is no more exclusively located in the center of the network. But, it is spread to the edge. In this model, users control their own privacy and rather than being controlled by a centralized authority. Devices are the master, the role of the cloud changes from a controller to that of a peer service provider (i.e. what IBM refers to as new and flat devices democracy where Devices and the cloud become equal citizens). This shift will require researchers to fundamentally rethink security mechanisms, by mainly building access control models and protocols with more privacy and autonomy.
- **Decentralized authorization and access control in trustless network like Bitcoin and Blockchain**: Decentralization and openness of Bitcoin protocol [131], which has no single point of trust or failure can lead to a whole wave of IoT innovations. We list below some use cases exploring blockchain technology in security and IoT field: (1) DOAuth (decentralized OAuth): to avoid OAuth concentrating identity to trust hubs (like Facebook, Google, etc.), authors propose decentralizing identity and authorizations to trustless networks (like Bitcoin and Blockchain). (2)Authors in [132,133] introduce FairAccess framework as a balance solution and equilibrium that solve the dilemma of centralized and decentralized access control management challenges highlighted above by leveraging the blockchain technology. (3) Adept protocol [134]: IBM has

spearheaded in CES 2015 the proof of concept of a new protocol called ADEPT which is a promising technology that combined Ethereums [135] blockchain-based decentralized platform programming language with BitTorrent and some code called Telehash to create an entirely new framework for building software for the Internet of Things. Conceiving an access control model for the described framework would be a worthwhile project.

- **Security on chip (hardware level)**: We recognize that IoT may provide an opportunity for hardware-based security thanks to the fast evolution towards a more powerful computing and memory in tiny device. Most hardware vendors and even software ones had realized that they need to have security solution in a chipset level. They have already started designing their hardware with security in mind. We list as example the most relevant innovation in this direction: (1) Vault project : On the second day of Googles annual conference for developers, the company has announced Project Vault. It looks at the thorny issue of encryption and security of mobile data. Vault consists of a micro SD card that contains all the elements to encrypt data or real-time communications on any device. The card works autonomously. It introduces new ways to communicate securely without the need for entering passwords. There is no doubt that this kind of engine will make the implementation of complex access control model in the constrained device side a reality. (2) Access control shield: building an access control shield by implementing OAuth protocol as example on IoT devices like Arduino, Raspberry Pi, Beagelbone, etc. would be an interesting project.
- **Security through transparency**: Current security models based on closed source approaches (often described as security through obscurity) are obsolete and must be replaced by a newer approach security through transparency. For this, a shift to open source is required. while open source systems may still be vulnerable to accidents and exploitable weaknesses, they are less susceptible to government and other targeted intrusion, for which home automation, connected cars and the plethora of other connected devices present plenty of opportunities.

7. Conclusion

Recently, many efforts have overcome many of the technological requirements for the integration of smart objects into the current Internet. However, IoT paradigm has still to face hard challenges related to the application of security and access control mechanisms over constrained environments. In this survey, we have established a taxonomy of IoT domain applications, ranging from big industries such as smart grid, to personal and everyday appliance such as smart homes. Furthermore, an OM-AM analysis of authorization process in IoT was provided. We have also extracted the pros and cons of existing access control solutions from an IoT perspective and their usability in the IoT domain applications already defined. We evaluated related literature in both quantitative and qualitative ways based on main IoT security requirements. This evaluation is highlighted with graph that shows in a very representative way how each model meets each requirement. On the light of our evaluation, we identified the main challenges of applying access control mechanisms to IoT and argued that commonly used Internet protocols cannot in every case be applied to constrained environments. We also discussed the main advantages and drawbacks of adopting a distributed or centralized access control management in IoT. Finally, based on latest innovations in IoT field, we have dressed the main future directions of security and particularly those of access control in IoT. Future work consists in implementing a privacy-preserving access control framework based on the presented OM-AM reference model in order to conceive an adequate access control framework for IoT.

References

[1] H. Mousannif, I. Khalil, in: The Human Face of Mobile, Springer, Berlin, Heidelberg, 2014, pp. 1–20, doi:10.1007/978-3-642-55032-4_1. http://link.springer.com/10.1007/978-3-642-55032-4_1.

[2] Orange, the future of digital trust a European study on the nature of consumer trust and personal data, Technical Report, 2014.

[3] Part2: Security functional components, in: Common Criteria Inf. Technol. Secur. Eval. 3.1 Revis. 1, p. 314.

[4] Part 1: Introduction and general model, in: Common Criteria Inf. Technol. Secur. Eval., version 3. edition, p. 86.

[5] H. Maw, H. Xiao, B. Christianson, J. Malcolm, A survey of access control models in wireless sensor networks, J. Sens. Actuator Networks 3 (2) (2014) 150–180, doi:10.3390/jsan3020150. http://www.mdpi.com/2224-2708/3/2/150/.

[6] S. Sicari, A. Rizzardi, L. Grieco, A. Coen-Porisini, Security, privacy and trust in internet of things: the road ahead, Comput. Networks 76 (2014) 146–164, doi:10.1016/j.comnet.2014.11.008. http://www.sciencedirect.com/science/article/pii/S1389128614003971.

[7] L. Atzori, A. Iera, G. Morabito, The internet of things: a survey, Comput. Networks 54 (15) (2010) 2787–2805, doi:10.1016/j.comnet.2010.05.010. http://linkinghub.elsevier.com/retrieve/pii/S1389128610001568.

[8] D. Miorandi, S. Sicari, F.D. Pellegrini, I. Chlamtac, Internet of things: vision, applications and research challenges, Ad Hoc Netw. (2012). https://sci-hub.io/http://www.sciencedirect.com/science/article/pii/S1570870512000674.

[9] R.H. Weber, Internet of things new security and privacy challenges, Comput. Law Secur. Rev. 26 (1) (2010) 23–30, doi:10.1016/j.clsr.2009.11.008.

[10] Z. Yan, P. Zhang, A.V. Vasilakos, A survey on trust management for internet of things, J. Netw. Comput. Appl. 42 (2014) 120–134, doi:10.1016/j.jnca.2014.01.014. http://dx.doi.org/10.1016/j.jnca.2014.01.014

[11] R. Roman, J. Zhou, J. Lopez, On the features and challenges of security and privacy in distributed internet of things, Comput. Networks 57 (10) (2013) 2266–2279, doi:10.1016/j.comnet.2012.12.018. http://dx.doi.org/10.1016/j.comnet.2012.12.018

[12] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of things (IoT): a vision, architectural elements, and future directions, Futur. Gener. Comput. Syst. 29 (7) (2013) 1645–1660, doi:10.1016/j.future.2013.01.010.

[13] A. Ouaddah, H. Mousannif, A. Ait Ouahman, Access control models in IoT: the road ahead, in: 2015 IEEE/ACS 12th Int. Conf. Comput. Syst. Appl., IEEE, 2015, pp. 1–2. http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7507090, 10.1109/AICCSA.2015.7507090

[14] A. Ouaddah, H. Mousannif, A. Abou Elkalam, Anas Ait Ouahman, Access control in IoT : survey & state of the art, in: 5th Int. Conf. Multimed. Comput. Syst. IEEE Conf., Marrakech, Morocco,

[15] P. Samarati, S.D.C. Di Vimercati, Access control: policies, models, and mechanisms, Found. Secur. Anal. Des. 2171 (2001) 137–196, doi:10.1007/3-540-45608-2_3. http://www.springerlink.com/index/80wrewj7j1a716wb.pdf

[16] J. Vollbrecht, P. Calhoun, S. Farrell, L. Gommans, G. Gross, B. de Bruijn, C. de Laat, M. Holdrege, D. Spence, AAA Authorization Framework, 2000 (No. RFC 2904).

[17] Boyle, D., Newe, T. (2007). A Survey of Authentication Mechanisms.

[18] V. Suhendra, A survey on access control deployment, Commun. Comput. Inf. Sci. 259 CCIS (2011) 11–20, doi:10.1007/978-3-642-27189-2_2.

[19] C. Alberts, A. Dorofee, J. Stevens, Introduction to the OCTAVE approach, PA, Carnegie Mellon, 2003. http://www.itgovernanceusa.com/files/Octave.pdf.

[20] R.S. Sandhu, Role-based access control, Adv. Comput. 46 (1998) 237–286, doi:10.1016/S0065-2458(08)60206-5.

[21] Webfarmr.eu, XACML 3.0 enhancements, Nanoscale Res. Lett. 6 (1) (2011) 297, doi:10.1186/1556-276X-6-297. http://www.ncbi.nlm.nih.gov/pubmed/21711787

[22] D. Hardt, The OAuth 2.0 Authorization Framework, 2012. http://tools.ietf.org/html/rfc6749.html.

[23] R. Sandhu, Engineering Authority and Trust in Cyberspace: The OM-AM and RBAC Way (2000) 111–119. http://doi.acm.org/10.1145/344287.344309\nhttp://dl.acm.org/ft_gateway.cfm?id=344309&type=pdf. 10.1145/344287.344309.

[24] E. Yuan, J. Tong, Attributed based access control (ABAC) for Web services, in: IEEE Int. Conf. Web Serv., IEEE, 2005, doi:10.1109/ICWS.2005.25. http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1530847.

[25] A. Kalam, R. Baida, P. Balbiani, S. Benferhat, F. Cuppens, Y. Deswarte, A. Miege, C. Saurel, G. Trouessin, Organization based access control, in: Proc. POLICY 2003. IEEE 4th Int. Work. Policies Distrib. Syst. Networks, IEEE Comput. Soc, 2003, pp. 120–131, doi:10.1109/POLICY.2003.1206966. http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1206966.

[26] X. Zhang, F. Parisi-Presicce, R. Sandhu, J. Park, Formal model and policy specification of usage control, ACM Trans. Inf. Syst. Secur. 8 (4) (2005) 351–387, doi:10.1145/1108906.1108908. http://portal.acm.org/citation.cfm?doid=1108906.1108908

[27] J. Park, R. Sandhu, Towards usage control models: beyond traditional access control, in: Proc. seventh ACM Symp. Access Control Model. Technol. - SACMAT '02, ACM Press, New York, New York, USA, 2002, p. 57, doi:10.1145/507711.507722. http://portal.acm.org/citation.cfm?doid=507711.507722.

[28] J. Park, Usage control : a unified framework for next generation access control, 2003.

[29] P. Calhoun, M. Holdrege, D. Spence, RFC 2904 - AAA Authorization Framework, 2000. https://tools.ietf.org/pdf/rfc2904.pdf.

[30] ISO/IEC 10181-3:1996, Information technology – open systems interconnection – security frameworks for open systems: access control framework, 1996. https://www.iso.org/obp/ui/#iso:std:iso-iec:10181:-3:ed-1:v1:en.

[31] V. Suhendra, in: A Survey on Access Control Deployment, Springer, Berlin, Heidelberg, 2011, pp. 11–20, doi:10.1007/978-3-642-27189-2_2. http://link.springer.com/10.1007/978-3-642-27189-2_2.

[32] A.D. Brucker, L. Brügger, P. Kearney, B. Wolff, An approach to modular and testable security models of real-world health-care applications, in: Proc. 16th ACM Symp. Access Control Model. Technol. - SACMAT '11, ACM Press, New York, New York, USA, 2011, p. 133, doi:10.1145/1998441.1998461. http://portal.acm.org/citation.cfm?doid=1998441.1998461

[33] H. Hu, G.-J. Ahn, K. Kulkarni, Anomaly discovery and resolution in web access control policies, in: Proc. 16th ACM Symp. Access Control Model. Technol. - SACMAT '11, ACM Press, New York, New York, USA, 2011, p. 165, doi:10.1145/1998441.1998472. http://portal.acm.org/citation.cfm?doid=1998441.1998472

[34] Y. Ledru, N. Qamar, A. Idani, J.-L. Richier, M.-A. Labiadh, Validation of security policies by the animation of Z specifications, in: Proc. 16th ACM Symp. Access Control Model. Technol. - SACMAT '11, ACM Press, New York, New York, USA, 2011, p. 155, doi:10.1145/1998441.1998471. http://portal.acm.org/citation.cfm?doid=1998441.1998471

[35] S. De Capitani di Vimercati, S. Foresti, S. Jajodia, P. Samarati, in: Access Control Policies and Languages in Open Environments, Springer, US, 2007, pp. 21–58, doi:10.1007/978-0-387-27696-0_2. http://link.springer.com/10.1007/978-0-387-27696-0_2.

[36] H. Lockhart, Using XACML Policies as OAuth Scope1–6.

[37] E. Borgia, The internet of things vision: key features, applications and open issues, Comput. Commun. 54 (2014) 1–31, doi:10.1016/j.comcom.2014.09.008. http://dx.doi.org/10.1016/j.comcom.2014.09.008.

[38] a. Bartoli, J. Hern, On the ineffectiveness of today ' s privacy regulations for secure smart city networks, Proc. third IEEE Int. Conf. Smart Grid Commun. (SmartGridComm 2012) (2012) 1–6.

[39] A. Bartoli, J. Hern, J. Hernández-Serrano, M. Soriano, in: Security and Privacy in your Smart City, Smart City Council, 2011, pp. 1–6. http://www.cttc.cat/resources/doc/111108-security-privacy-smart-city-45521.pdf.

[40] E. Egozcue, D.H. Rodríguez, J.A. Ortiz, V.F. Villar, L. Tarrafeta, Annex II. Smart Grid Security April (2012) 71.

[41] V.J. Jincy, S. Sundararajan, Classification mechanism for IoT devices towards creating a security framework, Adv. Intell. Syst. Comput. 321 (2015) 265–277, doi:10.1007/978-3-319-11227-5_23. http://link.springer.com/10.1007/978-3-319-11227-5_23.

[42] P. Misra, Y. Simmhan, J. Warrior, Towards a practical architecture for the next generation internet of things, arXiv:1502.00797(2015). http://arxiv.org/abs/1502.00797

[43] N. Marquardt, S. Greenberg, Informing the design of proxemic interactions, IEEE Pervasive Comput. 11 (2) (2012) 14–23, doi:10.1109/MPRV.2012.15. http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6127852

[44] N. Fatema, R. Brad, Security requirements, counterattacks and projects in healthcare applications using WSNs - a review, International Journal of Computer Networking and Communication 2 (2) (2014) 1–9.

[45] F.S. Ferraz, C. Candido, B. Sampaio, C. André, G. Ferraz, G. Henrique, A. Catharina, L.D. Carvalho, Towards a smart city security model exploring smart cities elements based on nowadays solutions, ICSEA 2013, Eighth Int. Conf. Softw. Eng. Adv. (c) (2013) 546–550.

[46] Regulation (EU) No 910/2014 of the European Parliament and of the Council, On electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC 23 July 2014.http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv3AOJ.L_.2014.257.01.0073.01.ENG

[47] Z. Yan, S. Holtmanns, Trust modeling and management: from social trust to digital trust, IGI Glob. (2008). https://books.google.com/books?hl=fr&lr=&id=wcWeBQAAQBAJ&oi=fnd&pg=PA279&dq=Trust+modeling+and+management:+from+social+trust+to+digital+trust&ots=2NS8t0SAhG&sig=wFrRiWDYAhaIzIA8-czZ1fV_VpY.

[48] A. Pfitzmann, M. Köhntopp, in: Anonymity, Unobservability, and Pseudonymity A Proposal for Terminology, Springer, Berlin, Heidelberg, 2001, pp. 1–9, doi:10.1007/3-540-44702-4_1. http://link.springer.com/10.1007/3-540-44702-4_1.

[49] ISO, IS 15408, 1999, http://www.commoncriteria.org/.

[50] G. Zhang, J. Tian, An extended role based access control model for the internet of things, 2010 International Conference on Information, Networking and Automation (ICINA), 1, IEEE, 2010, pp. V1–319.

[51] P. Spiess, S. Karnouskos, D. Guinard, D. Savio, O. Baecker, L.M.S. de Souza, V. Trifa, SOA-based integration of the internet of things in enterprise services, in: 2009 IEEE Int. Conf. Web Serv., IEEE, 2009, pp. 968–975, doi:10.1109/ICWS.2009.98. http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5175920

[52] L.M.S. deSouza, P. Spiess, D. Guinard, M. Köhler, S. Karnouskos, D. Savio, in: SOCRADES: A Web Service Based Shop Floor Integration Infrastructure, Springer, Berlin, Heidelberg, 2008, pp. 50–67, doi:10.1007/978-3-540-78731-0_4. http://link.springer.com/10.1007/978-3-540-78731-0_4.

[53] J. Jindou, Q. Xiaofeng, C. Cheng, Access control method for web of things based on role and SNS, in: 2012 IEEE 12th Int. Conf. Comput. Inf. Technol., IEEE, 2012, pp. 316–321, doi:10.1109/CIT.2012.81. http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6391920.

[54] E. Barka, S.S. Mathew, Y. Atif, in: Securing the Web of Things with Role-Based Access Control, Springer International Publishing, 2015, pp. 14–26, doi:10.1007/978-3-319-18681-8_2. http://link.springer.com/10.1007/978-3-319-18681-8_2.

[55] A. Soni, S.L. Keoh, S.S. Kumar, O. Garcia-Morchon, HADA: Hybrid Access Decision Architecture for Building Automation and Control Systems, Proceedings of the 1st International Symposium on ICS & SCADA Cyber Security Research 2013, BCS, 2013, pp. 1–11.

[56] J. Liu, Y. Xiao, C.P. Chen, Authentication and access control in the internet of things, in: 2012 32nd Int. Conf. Distrib. Comput. Syst. Work., IEEE, 2012, pp. 588–592, doi:10.1109/ICDCSW.2012.23. http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6258209.

[57] N. Sakimura, J. Bradley, M. Jones, B. de Medeiros, C. Mortimore, OpenID Connect Core 1.0, 2014. http://openid.net/specs/openid-connect-core-1_0.html.

[58] W.W. Smari, P. Clemente, J.-F. Lalande, An extended attribute based access control model with trust and privacy: application to a collaborative crisis management system, Futur. Gener. Comput. Syst. 31 (2014) 147–168, doi:10.1016/j.future.2013.05.010. http://www.sciencedirect.com/science/article/pii/S0167739X1300109X.

[59] N. Ye, Y. Zhu, R.-c. Wang, R. Malekian, L. Qiao-min, An efficient authentication and access control scheme for perception layer of internet of things, Appl. Math. Inf. Sci. An Int. J. 1624 (4) (2014) 1617–1624.

[60] A. Lazouski, F. Martinelli, P. Mori, Usage control in computer security: a survey, Comput. Sci. Rev. 4 (2) (2010) 81–99, doi:10.1016/j.cosrev.2010.02.002. http://dx.doi.org/10.1016/j.cosrev.2010.02.002.

[61] X. Zhang, M. Nakae, M.J. Covington, R. Sandhu, Toward a usage-based security framework for collaborative computing systems, ACM Trans. Inf. Syst. Secur. 11 (1) (2008) 1–36, doi:10.1145/1330295.1330298. http://portal.acm.org/citation.cfm?doid=1330295.1330298.

[62] G. Zhang, W. Gong, The research of access control based on UCON in the internet of things, J. Softw. (2011). http://ojs.academypublisher.com/index.php/jsw/article/view/4183.

[63] J.B. Dennis, E.C. Van Horn, Programming semantics for multiprogrammed computations, Commun. ACM 9 (3) (1966) 143–155, doi:10.1145/365230.365252. http://portal.acm.org/citation.cfm?doid=365230.365252.

[64] B. Lampson, Protection, ACM SIGOPS Oper. Syst. Rev. (1974). http://dl.acm.org/citation.cfm?id=775268.

[65] R. Sandhu, The typed access matrix model, in: Proc. 1992 IEEE Comput. Soc. Symp. Res. Secur. Priv., IEEE Comput. Soc. Press, 1992, pp. 122–136, doi:10.1109/RISP.1992.213266. http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=213266.

[66] T. Close, ACLs don't (2009). http://www.hpl.hp.com/techreports/2009/HPL-2009-20.pdf?q=dont.

[67] E. FP7, IoT@Work project, http://iot-at-work.eu.

[68] L. Gong, A secure identity-based capability system, in: Secur. Privacy, 1989. Proceedings, 1989, IEEE, 1989. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=36277.

[69] P. Mahalle, Identity authentication and capability based access control (IACAC) for the internet of things, J. Cyber Secur. Mobility 1 (2013) 309–348. http://forskningsbasen.deff.dk/Share.external?sp=S72df67ac-3ea5-41da-8cf0-523c6f71bbf2&sp=Saau.

[70] B. Anggorojati, P.N. Mahalle, N.R. Prasad, R. Prasad, Capability-based access control delegation model on the federated IoT network, in: 2012 15th Int. Symp. Wirel. Pers. Multimed. Commun. (WPMC), 2012, pp. 604–608.

[71] B. Anggorojati, P. Mahalle, N. Prasad, Secure access control and authority delegation based on capability and context awareness for federated IoT, Internet of Things, 2013. https://books.google.com/books?hl=fr&lr=&id=NnzoT5BofEoC&oi=fnd&pg=PA135&dq=secure+access+control+and+authority+delegation+based+on+capability+and+context+awareness+for+federaed+IoT&ots=fH8ro8_yHU&sig=PW0XGERXFr3WNgO6uiRvJ8BAWJ0.

[72] S. Gusmeroli, S. Piccione, D. Rotondi, A capability-based security approach to manage access control in the internet of things, Math. Comput. Model. 58 (5–6) (2013) 1189–1205, doi:10.1016/j.mcm.2013.02.006. http://dx.doi.org/10.1016/j.mcm.2013.02.006.

[73] T. Jacobs, IOT i IoT Reference Model White Paper, 2012.

[74] G.D. Skinner, Cyber security management of access controls in digital ecosystems and distributed environments, in: 6th Int. Conf. Inf. Technol. Appl., 2009, pp. 9–12.

[75] J.L. Hernández-Ramos, A.J. Jara, L. Marín, A.F.S. Gómez, DCapBac: embedding authorization logic into smart things through ECC optimizations, Int. J. Comput. Math. (March 2015) (2014) 1–22, doi:10.1080/00207160.2014.915316. http://www.scopus.com/inward/record.url?eid=2-s2.0-84900896844&partnerID=tZOtx3y1.

[76] J. Hernández-Ramos, A. Jara, Distributed capability-based access control for the internet of things, J. Internet Serv. Inf. Secur. 3 (2013) 1–16. http://isyou.info/jisis/vol3/no34/jisis-2013-vol3-no34-01.pdf.

[77] Z. Shelby, K. Hartke, B. C, The constrained application protocol (coap), 2014.

[78] S. Hui, Jonathan, Culler, David, Chakrabarti, 6LoWpan: incorporating IEEE 802.15. 4 into the IP architecture, IPSO Alliance White Pap. 3 (2009).

[79] J. Bernal Bernabe, J.L. Hernandez Ramos, A.F. Skarmeta Gomez, TACIoT: multidimensional trust-aware access control system for the internet of things, Soft Comput. 20 (5) (2016) 1763–1779, doi:10.1007/s00500-015-1705-6. http://link.springer.com/10.1007/s00500-015-1705-6.

[80] A. Kalam, R. Baida, P. Balbiani, S. Benferhat, F. Cuppens, Y. Deswarte, A. Miege, C. Saurel, G. Trouessin, Organization based access control, in: Proc. POLICY 2003. IEEE 4th Int. Work. Policies Distrib. Syst. Networks, IEEE Comput. Soc, 2003, pp. 120–131, doi:10.1109/POLICY.2003.1206966. http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1206966.

[81] A.E. Kalam, Y. Deswarte, Multi-Orbac: a new access control model for distributed, heterogeneous and collaborative systems, in: 8th IEEE International Symposium on Systems and Information Security, 2006, p. 1. http://homepages.laas.fr/deswarte/Publications/06427.pdf

[82] A. Abou El Kalam, Y. Deswarte, A. Baïna, M. Kaâniche, PolyOrBAC: a security framework for critical infrastructures, Int. J. Crit. Infrastruct. Prot. 2 (4) (2009) 154–169.

[83] A. Ouaddah, I. Bouij-Pasquier, A. Abou Elkalam, A. Ait Ouahman, Security analysis and proposal of new access control model in the Internet of Thing, in: 2015 Int. Conf. Electr. Inf. Technol., IEEE, 2015, pp. 30–35, doi:10.1109/EITech.2015.7162936. http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7162936.

[84] I. Bouij-Pasquier, A.A. El Kalam, A.A. Ouahman, M. De Montfort, in: A Security Framework for Internet of Things, Springer International Publishing, 2015, pp. 19–31, doi:10.1007/978-3-319-26823-1_2. http://link.springer.com/10.1007/978-3-319-26823-1_2.

[85] V. Tsiatsis, A. Gluhak, T. Bauge, F. Montagut, J. Bernat, M. Bauer, C. Villalonga, P. Barnaghip, S. Krco, The SENSEI real world internet architecture, Towards Future Internet Emerg. Trends from Eur. Res. (March) (2010) 247–256, doi:10.3233/978-1-60750-539-6-247.

[86] L. Scale, C. Project, SENSEI Integrating the Physical with the Digital World of the Network of the Future FP7 Contract Number : 215923 WP4 Efficient Wireless Sensor and Actuator Networks, Contract, 2008.

[87] T. Baugé, C. Sorge, A. Waller, G. Selander, SENSEI Internal Report IR3.5: Security and accounting for SENSEI,2010.

[88] P.N. Mahalle, P.A. Thakre, N.R. Prasad, R. Prasad, A fuzzy approach to trust based access control in internet of things, in: Wirel. VITAE 2013, IEEE, 2013, pp. 1–5, doi:10.1109/VITAE.2013.6617083. http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6617083.

[89] R. Neisse, I.N. Fovino, G. Baldini, V. Stavroulaki, P. Vlacheas, R. Giaffreda, A model-based security toolkit for the internet of things, in: 2014 Ninth Int. Conf. Availability, Reliab. Secur., 2014, pp. 78–87, doi:10.1109/ARES.2014.17. http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6980266.

[90] P. Vlacheas, R. Giaffreda, V. Stavroulaki, D. Kelaidonis, V. Foteinos, G. Poulios, P. Demestichas, A. Somov, A. Biswas, K. Moessner, Enabling smart cities through a cognitive management framework for the internet of things, IEEE Commun. Mag. 51 (6) (2013) 102–111, doi:10.1109/MCOM.2013.6525602. http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6525602.

[91] R. Neisse, G. Steri, G. Baldini, Enforcement of Security Policy Rules for the Internet of Things.

[92] IBM, MQ Telemetry Transport (MQTT) V3.1 Protocol specification, http://www.ibm.com/developerworks/library/ws-mqtt/.

[93] G. Baldini, M. Botterman, R. Neisse, M. Tallacchini, Ethical design in the internet of things, Sci. Eng. Ethics (2016) 1–21, doi:10.1007/s11948-016-9754-5. http://link.springer.com/10.1007/s11948-016-9754-5.

[94] A. Kannan, A. Abd El-Aziz, A comprehensive presentation to XACML, in: Third Int. Conf. Comput. Intell. Inf. Technol. (CIIT 2013), 2013, pp. 155–161, doi:10.1049/cp.2013.2585. http://digital-library.theiet.org/content/conferences/10.1049/cp.2013.2585.

[95] J.E. Kim, G. Boulos, J. Yackovich, T. Barth, C. Beckel, D. Mosse, Seamless integration of heterogeneous devices and access control in smart homes, in: 2012 Eighth Int. Conf. Intell. Environ., 2012, pp. 206–213, doi:10.1109/IE.2012.57. http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6258524.

[96] L. Seitz, G. Selander, C. Gehrmann, Authorization framework for the internet-of-things, 2013 IEEE 14th Int. Symp. a World Wireless, Mob. Multimed. Networks, WoWMoM 2013, 2013, doi:10.1109/WoWMoM.2013.6583465.

[97] M. Eve, M. Prateek, P. Rob, Assertions and Protocol for the OASIS 3 Security Assertion Markup Language 4 (SAML) V1.1, Technical Report, OASIS, 2003. https://www.oasis-open.org/committees/download.php/3406/oasis-sstc-saml-core-1.1.pdf.

[98] E. Hammer-Lahav, The OAuth 1.0 Protocol, 2010.

[99] E.A.K. Goud, M.J. Reddy, A survey on open authorization (OAuth) 1 (11) (2013) 110–114. https://tools.ietf.org/pdf/rfc5849.pdf.

[100] Facebook, Inc. Facebook authentication for websites, 2010, http://developers.facebook.com.

[101] Goggle, Inc. Google OAuth 2.0 (2011). http://code.google.com/apis/accounts/docs/OAuth2Login.html.

[102] Microsof, Inc. Microsoft Live Connect. http://msdn.microsoft.com/enus/windowslive/default.aspx.

[103] L. Seitz, G. Selander, E. Wahlstroem, S. Erdtman, H. Tschofenig, Authorization for the Internet of Things using OAuth 2.0, 2016, https://tools.ietf.org/html/draft-ietf-ace-oauth-authz-01.

[104] R. American Society of Heating, A.-C. E. (ASHRAE), BACnet - A Data Communication Protocol for Building Automation and Control Networks, 2009,. http://www.bacnet.org/Bibliography/EC-9-97/EC-9-97.html.

[105] B. Project, Building as a Service project, http://www.baas-itea2.eu/cms/

[106] D. Guinard, A web of things application architecture - integrating the real–world into the web, 2011. ETH Zurich, 19891

[107] P. Fremantle, B. Aziz, J. Kopeck, P. Scott, Federated Identity and Access Management for the Internet of Things, 1–8.

[108] P. Fremantle, J. Kopecký, B. Aziz, in: Web API Management Meets the Internet of Things, Springer International Publishing, 2015, pp. 367–375, doi:10.1007/978-3-319-25639-9_49. http://link.springer.com/10.1007/978-3-319-25639-9_49.

[109] N. Sakimura, J. Bradley, M. Jones, OpenID connect dynamic client registration 1.0(2011). http://openid.net/specs/openid-connect-registration-1_0-final.html.

[110] S. Cirani, M. Picone, P. Gonizzi, L. Veltri, G. Ferrari, IoT-OAS: An oauth-based authorization service architecture for secure services in IoT scenarios, IEEE Sens. J. 15 (2) (2015) 1224–1234, doi:10.1109/JSEN.2014.2361406.

[111] F.E. Project, Connect All IP-Based Smart Objects (CALIPSO), http://www.ict-calipso.eu.

[112] S. Cirani, M. Picone, Effective authorization for the web of things, in: 2015 IEEE 2nd World Forum Internet Things, IEEE, 2015, pp. 316–320, doi:10.1109/WF-IoT.2015.7389073. http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7389073.

[113] H. Tschofenig, E. Maler, E. Wahlstroe, E. S, Authentication and Authorization for Constrained Environments Using OAuth and UMA, 2015, draft-maler-ace-oauth-uma-00.txt

[114] D. Cabarkapa, Authorization Architecture for SWoT Authorization Architecture for SWoT.

[115] Ericsson, The Social Web of Things, 2011, https://www.youtube.com/watch?v=1syj_2jfJ4g.

[116] D. Rivera, L. Cruz-Piris, G. Lopez-Civera, E. de la Hoz, I. Marsa-Maestre, Applying a unified access control for IoT-based intelligent agent systems, in: 2015 IEEE 8th Int. Conf. Serv. Comput. Appl., IEEE, 2015, pp. 247–251, doi:10.1109/SOCA.2015.40. http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7399119.

[117] V. Varadharajan, S. Bansal, in: Data Security and Privacy in the Internet of Things (IoT) Environment, Springer International Publishing, 2016, pp. 261–281, doi:10.1007/978-3-319-33124-9_11. http://link.springer.com/10.1007/978-3-319-33124-9_11.

[118] W.V. Sujansky, S.A. Faus, E. Stone, P.F. Brennan, A method to implement fine-grained access control for personal health records through standard relational database queries, J. Biomed. Inform. 43 (5) (2010) S46–S50, doi:10.1016/j.jbi.2010.08.001. http://linkinghub.elsevier.com/retrieve/pii/S1532046410001115.

[119] H. Tschofenig, The OAuth 2.0 Bearer Token Usage over the Constrained Application Protocol (CoAP), 2016. https://tools.ietf.org/id/draft-moore-ace-oauth-observe-00.html.

[120] H. Tschofenig, The OAuth 2.0 Internet of Things (IoT) Client Credentials Grant, 2015, draft-wahlstroem-ace-oauth-introspection-01.txt 2015.

[121] E. Wahlstroem, OAuth 2.0 Introspection over the Constrained Application Protocol (CoAP), draft-wahlstroem-ace-oauth-introspection-01.txt 2015.

[122] H. Thomas, M. Eve, M. Machulak, D. Catalano, User-Managed Access (UMA) Profile of OAuth 2.0, 2015, https://docs.kantarainitiative.org/uma/rec-uma-core-v1_0_1.html.

[123] S.-T. Sun, K. Beznosov, The devil is in the (implementation) details: an empirical analysis of OAuth SSO systems, in: Proc. 2012 ACM Conf. Comput. Commun. Secur. - CCS '12, 2012, pp. 378–390, doi:10.1145/2382196.2382238.

[124] J. Schiffman, X. Zhang, S. Gibbs, DAuth: Fine-grained authorization delegation for distributed web application consumers, in: Proc. - 2010 IEEE Int. Symp. Policies Distrib. Syst. Networks, Policy 2010, 2010, pp. 95–102, doi:10.1109/POLICY.2010.12.

[125] R. Roman, C. Alcaraz, J. Lopez, N. Sklavos, Key management systems for sensor networks in the context of the internet of things, Comput. Electr. Eng. 37 (2) (2011) 147–159, doi:10.1016/j.compeleceng.2011.01.009.

[126] I. Leontiadis, C. Efstratiou, C. Mascolo, J. Crowcroft, SenShare: transforming sensor networks into multi-application sensing infrastructures, in: Proc. 9th Eur. Conf. Wirel. Sens. Networks, Springer-Verlag, 2012, pp. 65–81, doi:10.1007/978-3-642-28169-3_5. http://link.springer.com/10.1007/978-3-642-28169-3_5.

[127] W3C, Review of existing standards and their applicability,. https://www.w3.org/community/wot/wiki/Review_of_existing_standards_and_their_applicability.

[128] C. Neuman, T. Yu, S. Hartman, K. Raeburn, The Kerberos Network Authentication Service (V5), 2005.

[129] O. Vermesan, P. Friess, in: Internet of Things Strategic Research and Innovation Agenda Internet Things from Res. Innov. to Mark. Deploy., 2014, p. 143.

[130] K. Gusmeroli, S. Haller, S. Harrison, M. Kalaboukas, K. Tomasella, M. Vermesan, O. Wouters, Vision and challenges for realizing the internet of things, volume 1, 2009. 10.2759/26127.

[131] S. Nakamoto, Bitcoin : A Peer-to-Peer Electronic Cash System1–9..

[132] A. Ouaddah, A.A. Elkalam, A.A.I.T. Ouahman, Towards a novel privacy-preserving access control model based on blockchain technology in IoT 2 related work, in: Advances in Intelligent Systems and Computing, Eur. Middle East North Africa Conf. Technol. Secur. to Support Learn., Springer, Saidia, Morocco,

[133] A. Ouaddah, A.A. Elkalam, A.A.I.T. Ouahman, Harnessing the power of blockchain technology to solve IoT security & privacy issues, in: Second Int. Conf. Internet Things, Data Cloud Comput. (ICC 2017), in: ACM - International Conference Proceedings Series (ICPS), Cambridge City, United Kingdom, 2017.

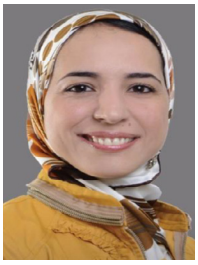
[134] S. Panikkar, S. Nair, P. Brody, V. Pureswaran, ADEPT : An IoT Practitioner Perspective(2015). http://ibm.biz/devicedemocracy.

[135] V. Buterin, A next-generation smart contract and decentralized application platform, Etherum (January) (2014) 1–36. http://buyxpr.com/build/pdfs/EthereumWhitePaper.pdf.

[136] J.B. Bernabe, J.L. Hernández, M.V. Moreno, A.F.S. Gomez, Privacy-preserving security framework for a social-aware internet of things, International Conference on Ubiquitous Computing and Ambient Intelligence, Springer International Publishing, 2014, pp. 408–415.

[137] A. Bassi, M. Bauer, M. Fiedler, T. Kramp, R. Van Kranenburg, S. Lange, S. Meissner, Enabling things to talk, Designing IoT Solutions With the IoT Architectural Reference Model (2013) 163–211.

Aafaf Ouaddah received the engineer degree in Networking and Information Technology in 2013, from the Telecommunications from the National Institute of Posts (INPT) GRADUATE SCHOOL ENGINEERING. Since 2014 she is a predoctoral researcher in the Department of Information and Communications Engineering at CADI AYYAD UNIVERSITY where she is pursuing a Ph.D. degree. Her main research interests are related to the design and implementation of novel security and privacy-preserving architecture and framework based on blockchain technology for the Internet of Things and fog commuting.



Hajar Mousannif is an assistant professor in the Department of Computer Science at the Faculty of Sciences Semlalia (Cadi Ayyad University, Morocco). She holds a Ph.D. degree in Computer Sciences on her work on wireless sensor networks and vehicular networks. She received an engineering degree in Telecommunications from the National Institute of Posts and Telecommunications (INPT), Rabat (Morocco) in 2005. Her primary research interests include Big Data, IoT, Human Computer Interaction, and next generation internet technologies. In addition to her academic experience, she was in the Technical Program Committee of many international conferences.

Anas Abou El Kalam is a university professor and president of the Moroccan Association of Digital Trust. He co-authored more than 150 papers and is certified ISO 27001 Lead Auditor, CEH (Certified Ethical Hacking) and CISSP (Certified Information Systems Security Professional). He was Assistant director of the OSCARS laboratory and in charge of the Networks, Systems and Security master as well as a former head of the Network and Telecommunication department at the UCA-ENSA. He also was an associate professor at the Institut National Polytechnique (INP) of Toulouse France where he obtained his HDR (Habilitation Diriger les Recherches) in security of critical networks and systems as well as his Ph.D. in security policies and models. He had several responsibilities as the Head of the Computer Science Department and the head of the Networks and Systems security Department at ENSIB (high school of engineers) France. He was invited professor at several universities in USA, Tunisia, Bucharest Technical Military Academy, etc. as well as a temporary professor at the Department of Defense training center in Bourges. His interest fields are Internet of Things security, Cloud security, critical systems security, access control models, evaluation of security mechanisms.

Abdellah Ait Ouahman was born in Marrakech, Morocco. He received the doctorate thesis in Signal Processing from the National Polytechnics Institute of Grenoble, France, in November 1981. His research was in Signal Processing and Telecommunications. In 1992, he received the PHD degree in Physics from the Faculty of Sciences in the Cadi Ayyad University, Marrakech, Morocco, He is now Professor and responsible of the OSCARS laboratory in the National School of Applied Sciences, Marrakech, His research interests include the signal and image processing and coding, telecommunications and networking.