Digital Communications and Networks 4 (2018) 118–137

Contents lists available at ScienceDirect

Digital Communications and Networks

journal homepage: www.keaipublishing.com/en/journals/digital-communications-and-networks/

A roadmap for security challenges in the Internet of Things

Arbia Riahi Sfar [a,b], Enrico Natalizio [b,*], Yacine Challal [c], Zied Chtourou [a]

[a] VRIT Lab - Military Academy, Nabeul, Tunisia
[b] Sorbonne Universites, Universite de technologie de Compiegne, CNRS, Heudiasyc UMR 7253, CS 60319, 60203 Compiegne Cedex, France
[c] Laboratoire de Methodes de Conception de Systemes (LMCS), Ecole Nationale Superieure d'Informatique (ESI), Centre de Recherche sur l'Information Scientifique et Technique (CERIST), Algiers, Algeria

ARTICLE INFO

Keywords:
Internet of Things
Systemic and cognitive approach
Security
Privacy
Trust
Identification
Access control

ABSTRACT

Unquestionably, communicating entities (*object*, or *things*) in the Internet of Things (IoT) context are playing an active role in human activities, systems and processes. The high connectivity of intelligent objects and their severe constraints lead to many security challenges, which are not included in the classical formulation of security problems and solutions. The Security Shield for IoT has been identified by DARPA (Defense Advanced Research Projects Agency) as one of the four projects with a potential impact broader than the Internet itself. To help interested researchers contribute to this research area, an overview of the IoT security roadmap overview is presented in this paper based on a novel cognitive and systemic approach. The role of each component of the approach is explained, we also study its interactions with the other main components, and their impact on the overall. A case study is presented to highlight the components and interactions of the systemic and cognitive approach. Then, security questions about privacy, trust, identification, and access control are discussed. According to the novel taxonomy of the IoT framework, different research challenges are highlighted, important solutions and research activities are revealed, and interesting research directions are proposed. In addition, current standardization activities are surveyed and discussed to the ensure the security of IoT components and applications.

1. Introduction

The long history of the Internet started in the 1950s following the development of electronic computers. Packet switched networks, such as the ARPANet (Advanced Research Projects Agency), were developed in the 1960s and 1970s, using a variety of protocols to join separate networks. In the 1980s, the TCP/IP(Transmission Control Protocol/Internet Protocol) Internet protocol suite was standardized, and the concept of the Internet as a worldwide network was introduced. In the 1990s, owing to the introduction of almost instantaneous communications, the Internet gave rise to a real revolution in everyday life, with domains as shown in a wide variety of popular networked applications.

The concept of the Internet of Things (IoT) was introduced in 1999 [1], after the explosion of the wireless devices market, and the introduction of the Radio Frequency Identification (RFID) and the Wireless Sensor Networks (WSN) technologies. The IoT concept aims to connect anything with anyone, anytime, and anywhere. It uses things or objects, e.g., sensors, actuators, RFID tags and readers, to enable interactions between the physical and virtual worlds. An illustrative example of an IoT application in a smart factory is shown in Fig. 1. In this system, we can distinguish four main components: person, process, technological ecosystem and intelligent object. The definitions, roles and interactions between these elements are given in Section 3.

In 2011, the number of interconnected systems exceeded the number of human beings [1]. In 2012, nine billion devices were interconnected; this number is expected to reach 24 billion devices in 2020 [1]. The size of the financial market approaches the amount of 1.3 trillion dollars for mobile network operators in various domains and applications such as healthcare, transportation, public services and electronics applications [1].

As an extension of the classical Internet framework and technology, previous security models should be applicable to IoT to guarantee basic security services including authentication, confidentiality, integrity, non-repudiation, access control and availability. However, the IoT is constrained by many new factors. First, numerous devices and objects may interact together in a complex manner, through many security techniques

* Corresponding author.
E-mail addresses: arbia.sfar@hds.utc.fr (A. Riahi Sfar), enrico.natalizio@hds.utc.fr (E. Natalizio), y_challal@esi.dz (Y. Challal), ziedchtourou@gmail.com (Z. Chtourou).

https://doi.org/10.1016/j.dcan.2017.04.003
Received 11 January 2017; Received in revised form 7 March 2017; Accepted 5 April 2017
Available online 13 April 2017
2352-8648/© 2017 Chongqing University of Posts and Telecommunications. Production and hosting by Elsevier B.V. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

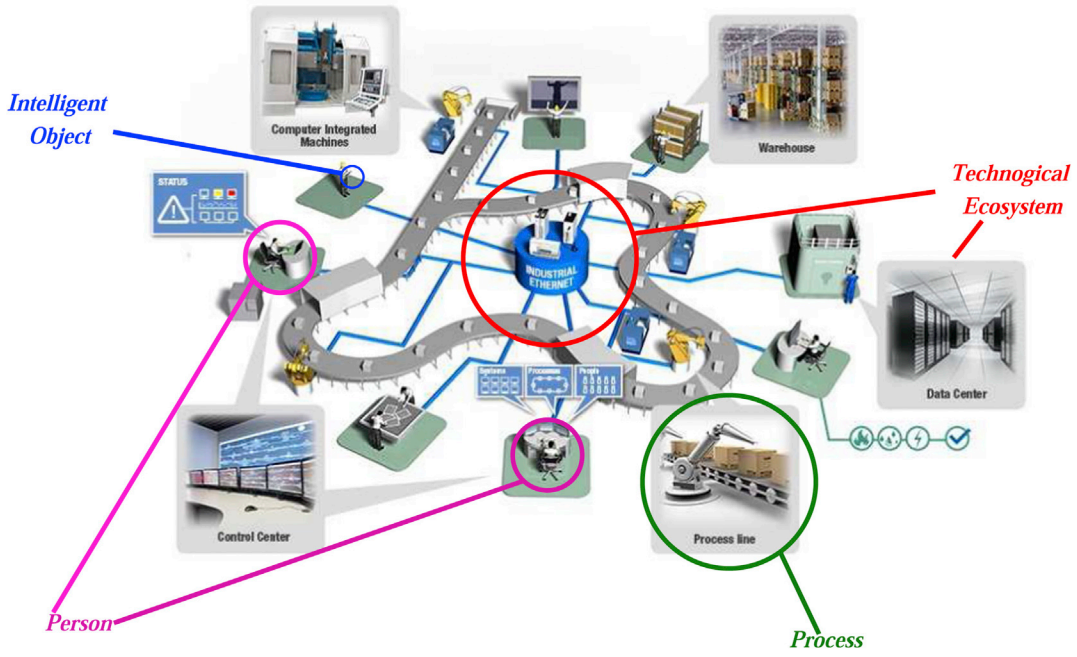


Fig. 1. A smart factory environment composed of *persons, smart objects, processes and a technological ecosystem* as the main elements of our systemic and cognitive approach for security in the Internet of Things. (©http://www.moxa.com).

and according to different policy requirements [2]. Second, IoT devices can have different operational environments and, usually, limited computational power. Third, some IoT have the potential for interaction with a huge number of nodes leading to serious security problems. Consequently, security challenges became more difficult to address as it is difficult to develop a generic "one size fits all" security strategy or model. The "Security Shield for Internet of Things" was identified in 2014 by DARPA (Defense Advanced Research Projects Agency) as one of the four projects with a potential impact broader larger than the Internet itself.

In addition, the evolution from closed or limited-access networks to open ones increased the need for security alarms to protect interconnected devices from intrusions. The IoT is susceptible to many types of attacks: message modification and/or alteration, traffic analysis, Denial of Service (DoS), Distributed DoS, eavesdropping, Sybil attacks, etc. Concretely, many real attacks occurred in the latest period. An example of an attack related to the IoT was led against Supervisory Control and Data Acquisition (SCADA) systems, which aim to facilitate the management of remote systems by issuing real-time supervisory commands over communication channels [3]. As a result of the commercial availability of cloud computing, these systems were progressively being used by IoT technology to decrease the infrastructure fees and facilitate maintenance and integration operations. In [3], the authors highlighted several security vulnerabilities and possible attacks of these systems (Denial of Service, SQL Injection, Buffer Overflow, and many others). The British Columbia Institute of Technologies Internet Engineering Lab (BCIT/IEL) has recorded a list of over than 120 events since the initiation of the project. Another analysis of 200 IT security executives using SCADA systems in different countries was led at McAfee enterprise, and showed that most facilities were victims of cyber-attacks [3].

Unquestionably, many challenging security issues must be addressed before making the IoT vision a reality. We need to answer important questions about enabling IoT while guaranteeing aspects such as trust, security, and privacy. We conducted this work to help those who are interested in the development and the improvement of this domain. Different surveys have already been proposed, but they are mainly based either on a broader vision that includes "Things"-oriented, "Internet"-oriented and "Semantic"-oriented visions, or on a layered vision, whereas the purpose of our work is to offer a roadmap that considers systemic and cognitive approach of IoT. This is useful especially when we consider the complexity, variability, interactions, and constraints of IoT components. Despite the limitations of its theoretical rigor, our vision remains an adequate choice for decision making, since we consider the overall system operation.

The main contribution of this work is fourfold: (a) we propose a classification of different surveys based on the IoT vision and security issues; (b) we detail our systemic and cognitive approach for the IoT, which was introduced in [4,5]; (c) we report and analyze the state-of-the-art of IoT security research activities, and present the major technological solutions and projects according to this systemic and cognitive approach; and (d) we show the main standardization activities related to IoT security. We believe that our effort is interesting as it grants particular attention to interactions among system elements and their effects on the overall system. Further, by using a systemic and cognitive approach, we consider the results originating from system behaviors and compare them to real-life results to validate models and practices.

Section 2 contains the related work, and highlights our contribution in respect of other existing surveys. Section 3 presents the systemic and cognitive approach of IoT that we use as a basis for our actual work. Section 4 shows how the presented model may be easily adapted to any real environment, by using it for smart manufacturing to improve productivity. Section 5 presents solutions and projects related to the IoT security field, which are classified according to different taxonomies, and, for each main research axis, highlights new research directions. Section 6 details the main standardization activities in the IoT security field. Section 7 discusses IoT security evolution and concludes the paper.

2. Related work

In recent years, many surveys were published to emphasize the advancement of research activities in the IoT framework [1,6–10]. They mainly focus on general issues of IoT fundamentals or models. Security concerns were presented as a part of each survey and treated in a generic manner and security and privacy were often shown jointly as a single concept. Unfortunately, as illustrated in Table 1, none of the previous surveys has detailed in-depth security concerns of the IoT.

Table 1
Surveys on Internet of Things.

Survey	Citation	Year	IoT vision	Security issues
The Internet of Things: A survey	[6]	2010	Things-oriented, Internet-oriented and Semantic-oriented	Identification, authentication, integrity, privacy, trust
Internet of Things: A Vision, Architectural Elements,and Future Directions	[1]	2012	Cloud centric vision	Identification, authentication, integrity, privacy
Internet of things: Vision, applications and research challenges	[7]	2012	anything communicates, anything is identified, and anything interacts	Data confidentiality, privacy, trust
The Internet of Things: A Survey from the Data-Centric Perspective	[8]	2013	Things-oriented, Internet-oriented and Semantic-oriented	Identification, integrity, privacy
Towards Internet of Things: Survey and Future Vision	[9]	2013	3-Layer architecture, 5-Layer architecture	Physical security, privacy
Context Aware Computing for The Internet of Things: A Survey	[10]	2013	Things to be connected Anytime, Anyplace, with Anything and Anyone, using Any path, network and Any service.	Identification, privacy, trust
Security for the Internet of Things: A Survey of Existing Protocols and Open Research issues	[12]	2015	5-Layer architecture	Authentication, integrity, confidentiality, trust, access control
Security, privacy and trust in Internet of Things: The road ahead	[13]	2015	A collection of smart devices that interact on a collaborative basis to fulfill a common goal	Privacy, trust, integrity, confidentiality, identification, authentication
Securing the Internet of Things Survey	[14]	2016	any-to-any connectivity	Authentication, access control, confidentiality
Internet of Things: A Review of Surveys Based on Context Aware Intelligent Services	[15]	2016	Different perspectives: services, connectivity, communication and networking viewpoints.	Privacy, integrity, access control, trust, identification.
Our work	–	–	Systemic and cognitive approach	Identification, access control, trust, privacy

In “The Internet of Things: A survey” [6], the authors aimed to present the different visions of the IoT paradigm: “Things”-oriented, “Internet”-oriented and “Semantic”-oriented visions. They reported the enabling technologies, including identification techniques, sensors and communication technologies and middleware features. Then, many applications of IoT are proposed in various fields, such as transportation, logistics, healthcare, smart environment, personal and social domains. From a security point of view, they focused on authentication and data integrity concerns, and proposed research directions for problems, such as a proxy attack and man-in-the-middle attack. Concerning privacy, they suggested to develop new software applications to control access to personal data during their life cycle. Although the survey is complete and interesting, it provides insufficient details about security challenges in the IoT.

In “Internet of things: Vision, applications and research challenges” [7], the authors considered that the IoT consists of three main levels: anything communicates, anything is identified, and anything interacts. They focused their research challenges on (1) computing, communication and identification technologies, (2) distributed systems technology, and (3) distributed intelligence. Miorandi et al. said that many challenges arise in security but they identified only three key issues to be innovated: data confidentiality, privacy and trust. They did not grant adequate attention to authentication, integrity and access control, which were discussed superficially and considered as parts of the key issues defined by the authors.

In “Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions” [1], the authors presented a cloud centric vision for the IoT and illustrated the enabling technologies and application domains of the future. They proposed many research issues based on [11]. The authors did not discuss security research issues in depth and their discussions were limited to superficial questions regarding privacy and identity protection.

In “The Internet of Things: A Survey from the Data-Centric Perspectiv” [8], the authors detailed data mining and management in the IoT according to the same visions as [6]. They focused essentially on (1) networking issues, including effects on data collection, RFID technology, sensor networks and mobile connectivity; and (2) data management and analysis, including data cleaning, semantic web, real-time and big data analysis, and crawling and searching the IoT. In this survey, security concerns were detailed only from a privacy point of view, and other relevant security issues were neglected.

In “Towards Internet of Things: Survey and Future Vision” [9], the authors proposed different architectures of the IoT, and discussed new research challenges. They detailed the 3-Layer and 5-Layer architectures and highlighted the relevant research challenges in communications problems (QoS, huge number of objects, transport control protocol, real time objects detection, etc.), and information gathering problems (massive information, and security and privacy problems). Authors were limited to physical security and privacy issues and they treated security problems superficially without presenting any possible solutions.

In “Context Aware Computing for The Internet of Things: A Survey” [10], the authors proposed a context awareness for the IoT framework and provided an in-depth analysis of the context life cycle (techniques, methods, models, functionalities, systems, applications, and middleware solutions) by studying a set of 50 projects during the decade between 2001 and 2011. Then, according to their taxonomy, they proposed a number of possible research directions based on emerging IoT issues. In this survey, the authors suggested that security and privacy issues are addressed at the middleware level, and at several layers of the model (sensor hardware, sensor data communication, context annotation and context discovery, context modeling and the context distribution layers) in order to gain trust from IoT users. This survey dealt with security as an orthogonal issue among many others, but no particular attention was paid to real research activities in this field.

In “Security for the Internet of Things: A Survey of Existing Protocols and Open Research issues” [12], published in 2015, Granjal et al. proposed a deep analysis of existing protocols and security mechanisms of communications in IoT and presented different open research issues. For their presentation, the authors adopted a standardized 5-layer protocol stack and considered security requirements and solutions for each layer. This work focused exclusively on security issues based on some standardization efforts performed by IEEE and IETF including IEEE 802.15.4, CoAP, 6loWPAN, RPL and CORE. Unfortunately, the authors neglected many other important standards in the same area, such as IoT-A reference model, P2413 (IEEE), oneM2M project, and ETSI efforts (TC M2M, and TC ITS) as explained in Section 6. Their work remained dependent on a limited number of standards and was not sufficiently open to other

efforts.

Another survey was published in 2015, by Sicari et al. entitled "Security, privacy and trust in Internet of Things: The road ahead" [13] in which the authors adopted an open IoT vision and considered a set of intelligent objects that cooperate to accomplish a common objective. In their vision, they considered that, from a technological point of view, IoT deployments may involve diverse conceptions, technologies, implementations and architectures to build a communication or to perform a process. They divided the security aspects into three categories: security requirements (authentication, confidentiality and access control), privacy, and trust. The main limitation of this work is the taxonomy of the IoT, which remains unclear and, consequently, the lack of classification of the listed research activities according to a clear sorting logic.

In 2016, the SANS institute published an interesting survey: "Securing the Internet of Things Survey" [14], to reveal the opinion of the security community about the IoT security state of the IoT in the present and in the future by interrogating security personnel active in the IT field. By the end of this survey, the author concluded that most of the respondents expected IoT device producers to show more interest in security concerns than other IT systems.

Finally, we cite the survey "Internet of Things: A Review of Surveys Based on Context Aware Intelligent Services" [15], which presented the current IoT technologies, approaches, and models to find out new data-related challenges. The paper proposed well integrated and context aware intelligent services for IoT. The authors focused on social network and IoT integration in the emerging context of the Social Internet of Things (SIoT). Although the security was considered by the authors during their survey, they did not discuss separately.

It is clear that all of the aforementioned surveys either did not consider security in the IoT framework as a priority or were limited to a part of its issues. In our work, we consider different IoT threats and focus on many areas, such as protocol and network security, data privacy, identity management, trust and governance, fault tolerance, dynamic trust, security, and privacy management. More than offering a classic survey, our intent is to present a roadmap for designers and practitioners of IoT to provide supplementary efforts in different and interesting areas to improve IoT security features. To this end, we proposed a systemic and cognitive approach for IoT security to cover all these aspects in a consistent framework [16]. Compared to the layered approach, our vision is more convenient and flexible for making decisions while the whole system accomplishes a given action. We consider security issues that may occur due to interactions among all the system elements, and analyze their consequences on the global system. We concentrate our analysis on specific interactions which are directly related to security: *privacy*, *trust*, *identification*, *and access control*. We consider that other interactions (*auto-immunity*, *safety*, *reliability and responsibility*) are considered during the system design phase, and do not involve enhancing technologies; and then remain beyond the scope of this work.

3. A systemic and cognitive approach for the IoT

In [5], the authors proposed a holistic view of the IoT suggesting a systemic and cognitive approach for the IoT security. The main idea is originally inspired by [17], where Kiely et al. proposed a systemic security management system for all types of organizations beginning with the micro level. As shown in Fig. 2, our illustration of the IoT context is described by a tetrahedron-shaped scheme built around four nodes: person, process, intelligent object, and technological ecosystem. The presence of the intelligent object in this system increases the complexity of the control process in the resulting computing environment which may include humans, computers, sensors, RFID tags, network equipment, communication protocols, system software, and applications. Edges between intelligent object and people nodes become difficult to process due to the large number of involved entities (objects and/or persons) and the varied of security requirements. These connections are dynamic and complex; follow the characteristics of the environment and play a key role of cooperation/conflict between nodes [16]. Nodes are connected to each other and their interactions are represented by seven edges: trust, privacy, identification and access control, safety, reliability, auto immunity, and responsibility. In the following, we provide a detailed definition of each of the nodes and edges of the tetrahedron. The relevant research issues are presented in Section 5.

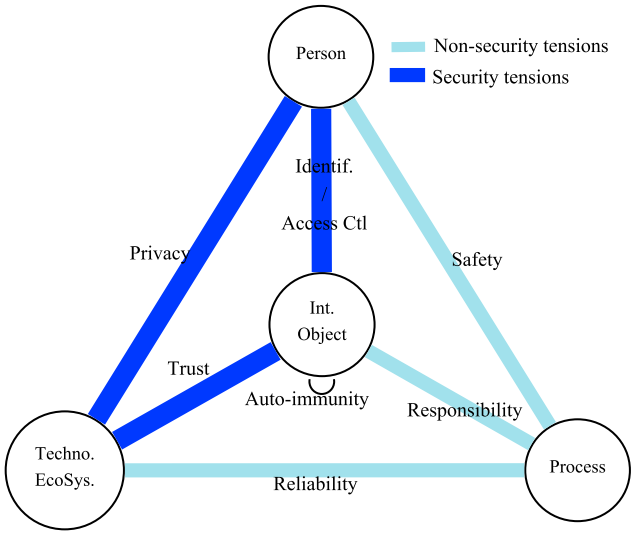


Fig. 2. Graphical illustration of IoT context according to its main elements (nodes) and their relationships (edges).

3.1. Nodes

3.1.1. Person

This node symbolizes the human resources and related security issues. As the IoT context is characterized by its diversity and large-scaled structure, security limitations and threats are more probable and influenced by large numbers of persons. When highlighting the complexity of this node, we need to aware that the persons involved include humans with different security background levels. This differs according to respective characters, manners, expertise, knowledge, outlook, etc. [17]. According to respective roles, different types of human profiles are involved in the IoT context, such as consumers, end users, and service or technology providers. Controlled by their security and safety, we suggest that persons, each from their perspective, have to accomplish the tasks related to security rules management, according to the Plan-Do-Check-Act approach described in the ISO/IEC 27000-series.[1]

3.1.2. Process

This node is about the procedures, means or ways to perform tasks within the IoT framework with respect to a specific security policy. Processes must thoroughly fit the requirements of policies, standards, strategies, procedures, and other specific documentation or regulation to guarantee the expected security level for every IoT architectural component.

3.1.3. Intelligent object

It encompasses various devices with communication capabilities regardless of their processing power, memory or energy as tags, sensors, actuators, etc. Objects can be deployed to work autonomously, as is the case of phase meters for a smart grid, or as part of a more complex system such as a thermostat in the HVAC (Heating Ventilation and Air Conditioning) system. The designers of these objects have to overcome their pervasive character to comply with specific security levels.

[1] http://www.27000.org/.

3.1.4. Technological ecosystem

This ecosystem represents technological solutions to guarantee efficient functioning and acceptable IoT security level, including joining applications, command and control processing, and routing and security. An extensive, reusable and accessible ecosystem is highly recommended to facilitate the development of IoT nodes and applications. To guarantee a generic and efficient secure technological ecosystem, the following aspects need to be considered: (1) design and configuration of security procedures, (2) identification and authorization of involved entities, (3) precision of internal and external security perimeters, and (4) protection of the physical environment. Practically, in the real implementation of a technological ecosystem, many issues have to be handled concerning communications infrastructures and protocols, system architecture, implemented algorithms, access control methods, etc have to be addressed. As data and commands may be remotely generated and handled, adequate interest needs to be granted to communication choices.

3.2. Edges

3.2.1. Privacy

It depicts the edge between person and technological ecosystem nodes and originates from the necessity of protecting data related to humans. In IoT, it is essential to fulfill privacy requirements due to the omnipresence of intelligent objects, and the risk of technology mishandling by legitimate and/or illegitimate users. For example, we consider a healthcare scenario where hospital employees need to access patient data for administrative purposes (statistics generation, patient registration, billing, age, sex…) and are not allowed to know details about patient disease. In this situation, privacy is about granting adequate access privileges to employees without divulging sensitive information.

3.2.2. Trust

It is the edge that links the intelligent object with the technological ecosystem. In smart environments, IoT devices may perform various readings (temperature, humidity, fire, pressure measurements, etc.) to pacilitate decision making by administrators and instant reaction. This reflects the necessity of trusting the involved device(s) to make the right assessment, and highlights the interaction between entities by trusting what they report and acting accordingly. Then, establishing and managing trust in a huge number of objects in heterogeneous and large-scaled environments is a considerable challenge for researchers and manufacturers. Trust management definition and operations (establishing, updating, and revoking credentials, keys and certificates) have to be addressed as a key security issue in IoT. In our approach, trust establishment between objects and persons is performed via technological ecosystems due to the involvement of human and non-human entities in the global system.

3.2.3. Identification/access control

It stands for the edge between persons and intelligent nodes, which emphasizes the mean to establish connections among entities, and retrieve them easily using their identifiers. We can consider the example of vehicle control in an industry chain where identifying connected devices (vehicles, products, etc.) permits their localization and tracking. Obviously, getting this type of information instantly can improve the global system functioning and efficiency by immediate intervention when needed. Identification affects many aspects of the global IoT system, including conception, architecture, access rules, etc.

3.2.4. Reliability

It links process and technological ecosystem nodes and depicts the probability of non-failure of the system operation. In IoT, reliability can be considered in many cases, such as handling unique and reliable addresses for entities, managing data over the network, and effective use of intelligent objects in various applications. In the systemic and cognitive approach, we classify reliability as a non-security edge as it is considered in the overall system designing. Although research efforts in IoT reliability are still limited, we can list two mains projects: NEBULA (A trustworthy, secure and evolvable Future Internet Architecture)[2] and Soft Reliability Project.[3]

3.2.5. Safety

It is largely about protecting persons and objects during a process execution. The software embedded into autonomous objects may be the cause of a random or unpredictable behavior so it has to be carefully checked to avoid disastrous consequences for the whole system and the physical environment. To explain the importance of safety in IoT domain, we consider the example of digital cities where smartphones are increasingly powerful tools that can be used as sensors. They must be capable to protect their internal and sensitive information and can predict and prevent safety issues through dedicated applications (e.g., geopositioning). Safety is also considered during the system design, which explains the limited related research efforts. Three main projects may be listed: E-Safety Project,[4] e-Crime Wales,[5] and Internet Safety Project.[6]

3.2.6. Auto-immunity

It concerns only intelligent objects as they may operate in remote and/or hostile zones where risks of physical attacks and other possible menaces become probable (failure of communication media, resource constraints, inadequate physical protection, weakness of the trust management system, sporadic nature of connectivity, etc). Strong electromagnetic disturbance may even interrupt or prevent the node from functioning. This increases the workload and battery consumption, which reduces the service time of the wireless sensors. Moreover, it is important to improve the IoT system immunity against electromagnetic interference to guarantee a low probability of both interception and low probability of detection [18]. Auto-immunity is concerned with all of the aforementioned aspects and needs to be considered as a conception requirement of every IoT system rather than a security measure. This edge is considered in the conception phase by manufacturers of IoT devices to ensure a prevention technique for intelligent objects and may explain the limited related research efforts. Two main works may be listed about artificial immunity-based security [19], and immunity-based intrusion detection technology [20].

3.2.7. Responsibility

It links the process to intelligent object nodes. Smart devices may be autonomous and behave as actors in many cases. For example, persons may grant a form of responsibility to these nodes to perform a precise action as responsibility for risk and vulnerabilities management of these products [21]. We consider a smart refrigerator, which is able to know the list of the stored aliments, and autonomously order new products. This device becomes responsible for product ordering which may facilitate the task of its proprietor. However, in the case of intentional or accidental dysfunction (poor products details, quantity problems, etc.), it is necessary to attribute the responsibilities to the right entities, and reactions may be taken accordingly.

In [16], a systemic and cognitive approach is developed through identification of contextual plans within the tetrahedron: a safety plan, cyber-security plan, access plan, and security plan; and the edges between nodes are sorted accordingly. It is then put into evidence by shedding light on the security plan that includes the privacy, trust, identification and access control edges. Each of the other plans of the tetrahedron (safety, access and cyber-security planes) share one edge

[2] http://www.nebula-fia.org/.
[3] http://www.softreliability.org/.
[4] http://www.em-esafetyproject.co.uk/.
[5] http://www.ecrimewales.com/.
[6] http://www.internetsafetyproject.org/.

with the security plan. Thus, we suggest a by-design inclusion of security in the different aspects of IoT development.

4. Case study: smart manufacturing

To highlight the efficiency of the systemic and cognitive approach, we consider the case of smart manufacturing, where IoT applications are expected to generate 1.2–3.7 trillion of economic value annually by 2025.[7] Concretely, IoT applications increase manufacturing productivity by providing a comprehensive view of the production chain and making instant adjustments. In the smart manufacturing scenario illustrated in Fig. 3, the nodes of the tetrahedron correspond to the following actors during the supply chain management process:

Process: the smart manufacturing process includes supply chain management, efficient operation, predictive maintenance and inventory optimization. Data collected from terminal equipment, workers, vehicles, and other sensors are analyzed to produce real-time models and control, and plan algorithms to coordinate between chain components. Monitoring the status of production equipment in real-time helps the increase of efficiency and reliability, and improve overall performance.

Person: to ensure the management of a large amount of heterogeneous data, manufacturing environment involves several actors with different competences and expertise. Depending on their interest, qualifications and ability to act in a reflective and autonomous way, persons needed in smart manufacturing context may be engineers, workers, managers, suppliers, consumers, tele-operators (conferencing, maintenance, etc.).

Intelligent object: devices involved in smart manufacturing include physical components (mechanical, electrical parts), intelligent components (sensors, actuators, microprocessors, software, and embedded operating systems) and connectivity components (wireless connectivity, ports, antennas). The explosion of sensor technologies has made every manufacturing process and component a potential data source. For example, sensors may be used to monitor humidity conditions during vehicle painting, and enable real-time monitoring by adjusting ventilation systems.

Technological ecosystem: innovations provide many opportunities to develop new products and corporate models, multiply economic benefits and facilitate greater employee engagement. In smart manufacturing, examples of these ecosystems may concern control technologies (sensors, actuators), cognition-based intelligence (machinery, robots), human-machine interaction, continuous monitoring, energy technologies, information and communication technologies, etc.

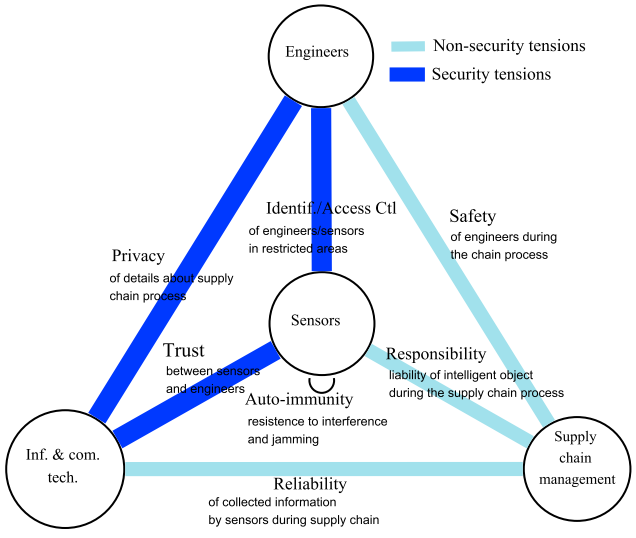


Fig. 3. Actors (nodes) and interactions (edges) in IoT context during supply chain management.

[7] http://www2.itif.org/.

Privacy: aims to reduce the risk of privacy disclosure of sensitive data (financial, technical or personal details) when exchanged with the technological ecosystem (radio link). Data control techniques such as anonymization, encryption, aggregation, integration, and synchronization, may be used to hide these data while providing essential information usable for the relevant applications.

Identification/Access control: consists of controlling illegitimate intrusions of persons/objects in restricted areas. It may concern identification and localization of vehicles, measurement of the humidity and temperature, tracking of products, management of surveillance parameters in sensitive areas, etc.

Trust: concentrates on soft security (technological ecosystem) to establish mutual trust between intelligent objects and persons, and create security guarantees and transparency. This enables the global system to make timely and trusted information available where it is needed, when it is needed, and to those who need it. Trust establishment will depend on two factors: the ability of an intelligent object to protect itself in hostile environments, and a person's ability to interrogate the node to determine whether it is still trustworthy.

Reliability: focuses on reliability of the information collected and the results reported by the technological ecosystem during the manufacturing process. This requires effective means of sensing, metrology, calibration, signal processing, diagnostics, anomaly detection, maintenance, etc. In addition, automatic, flexible and adaptive control mechanisms need to be developed to obtain a higher degree of the overall system reliability.

Safety: focuses on several operations, such as control, command, surveillance, communications, intelligence, and reconnaissance, etc. It aims to meet the need of intelligent objects, ensure their safety across their whole life cycle, and improve persons' safety by reducing injuries and fatalities during the manufacturing process. In this context, IoT may be applied to devices and employees (RFID tags, badges) to alert or even power off equipment if a physical attack occurs.

Auto-immunity: concerns the protection of intelligent objects from physical attack in harsh environments and providing the provision of sufficient resistance with the ability to self-monitor and reporting. It also focuses on enhanced immunity of intelligent objects and communication channels towards interference and jamming.

Responsibility: handles the liability of an intelligent object to perform a precise process. In a manufacturing scenario, IoT devices must answer only respond to an authorized reader's request. If a strategic change occurs, the responsibility for monitoring would change automatically, and responsibilities are distributed across multiple intelligent objects to perform new processes. Consequently, it is the responsibility of the whole system to maintain a consistent task agenda by inserting missing actions, guaranteeing general domain knowledge and causality, and so on.

5. Roadmap overview of security-related edges

In this section, we will survey security related edges: privacy, trust, identification and access control, present the current state of the art and propose possible research issues.

5.1. Privacy

Information privacy means that the user is able to control when, how, and to what extent personal information is collected, used, and shared. It can affect user confidence and people's lives. In an IoT environment, connected systems may communicate with each other, transmit collected, or control exchanged data. The capabilities of system's connections during various processes imply many security and privacy issues in the dynamic world of IoT, regarding constraints of maintaining the meaning of the handled information.

5.1.1. State of the art and taxonomy

In ubiquitous computing systems, sensitive data can be stored in a distributed manner. It is important to set up an adequate control mechanism, and control and manage data disclosure to third parties according to information sensitivity. Privacy for end-users is a very complex issue because it involves interactions with all of the different system components, and it cuts across all the layers of the systems structure. Obtaining and analyzing all these properties denotes a significant research challenge. Two comprehensive surveys about challenges and opportunities in big data privacy can be found in [22] and [23] where authors reviewed the milestones of research activities of big data privacy, and debated the challenges and opportunities from various perspectives.

To produce a consistent roadmap overview for the different research achievements and projects in IoT privacy concerns, we can distinguish two main axes: data privacy and access privacy, as illustrated in Fig. 5.

Data privacy must be considered throughout the different phases of data usage, including collection, transmission, and storage. During data collection and transmission, we need to focus on networking issues and technologies as RFID, WSN, and mobile connectivity. In the storage and processing phase at collection nodes, guaranteeing data confidentiality and integrity, and implementing adequate security techniques must take place. Effective solutions include anonymization, block ciphers, stream ciphers, hash functions, lightweight pseudo random number generator functions, and lightweight public key primitives. These techniques are generally combined to provide the required level of privacy depending on the sensitivity of data, network settings, and application and users requirements.

Access privacy emphasizes the manner in which people can access to personal information. It is important to highlight the need for efficient policies and mechanisms to manage different types of data and fit various situations in IoT contexts. This group may include blocking approaches, lightweight protocols and data sharing, and accessing techniques.

5.1.2. Data privacy

Important research results can be divided into six categories: anonymization based techniques, block ciphers, stream ciphers, hash functions, lightweight pseudo-random number generator functions, and lightweight public key primitives. Fig. 4 represents the chronological progress of research efforts in this domain (Fig. 5).

5.1.2.1. Anonymization-based solutions. These solutions aim to guarantee data privacy-preservation and include k-anonymity, l-diversity and t-closeness. K-anonymity focuses on the manner in which data holders can issue their private data without any risk of re-identification of data subjects. A formal protection model for sensitive data ensures that the information for each person cannot be differentiated from that belonging to a group of at least $(k-1)$ individuals [24,25].

The principle of k-anonymization consists of representing a database as a table with n rows and m columns. Each row denotes an entry associated with a precise member of the population, the entries are not necessarily unique. Columns of the table correspond to various attributes of different members of the population. To accomplish k-anonymity, two methods may be used: (1) suppression, where some values of the attributes are replaced by an asterisk '*'; and in one column, all or some values can be replaced by '*'; and (2) generalization, where personal values of attributes are replaced by values in a broader category (e.g., if the attribute 'age' is considered, the value of '21' can be replaced by the expression '≤ 25').

In IoT environments, k-anonymity may be used for the localization of intelligent objects to improve location privacy [26]. This can solve the security problems related to the use of a third party service for obfuscation, difficulty of managing several k-anonymity groups for different queries, and infeasibility of using global GPS coordinates indoors. Another proposal is to use a tree based location privacy approach against multi-precision continuous attacks, based on the new location query approach supporting multi-precision queries [26]. A third use of the k-anonymity concept was the case of building an algorithm for data release based on fine-grained generalization [27].

L-diversity is proposed to overcome k-anonymity vulnerability to homogeneity attack and background knowledge attack [28]. Machanavajjhala et al. proposed a stronger definition through well-represented sensitive attributes to guarantee privacy even when the data publisher ignored what the adversary knew about the records. A formal foundation was given and followed by an experimental evaluation and some practical directions of solution. In IoT, a possible application of this mechanism can be found in healthcare domain where data publication is needed without divulging sensitive information about individuals.

T-closeness was proposed in [29] to surmount limitations of k-anonymity and l-diversity related to attribute revelation. Li et al. proposal requires that distribution of sensitive attributes in any group should be close to their distribution in the overall database. To highlight the value of this work, the authors use real examples and experiments. In [30], the authors present a decomposition with (n-t) closeness to maintain privacy in the case of multiple sensitive attributes. Their goal was to solve the

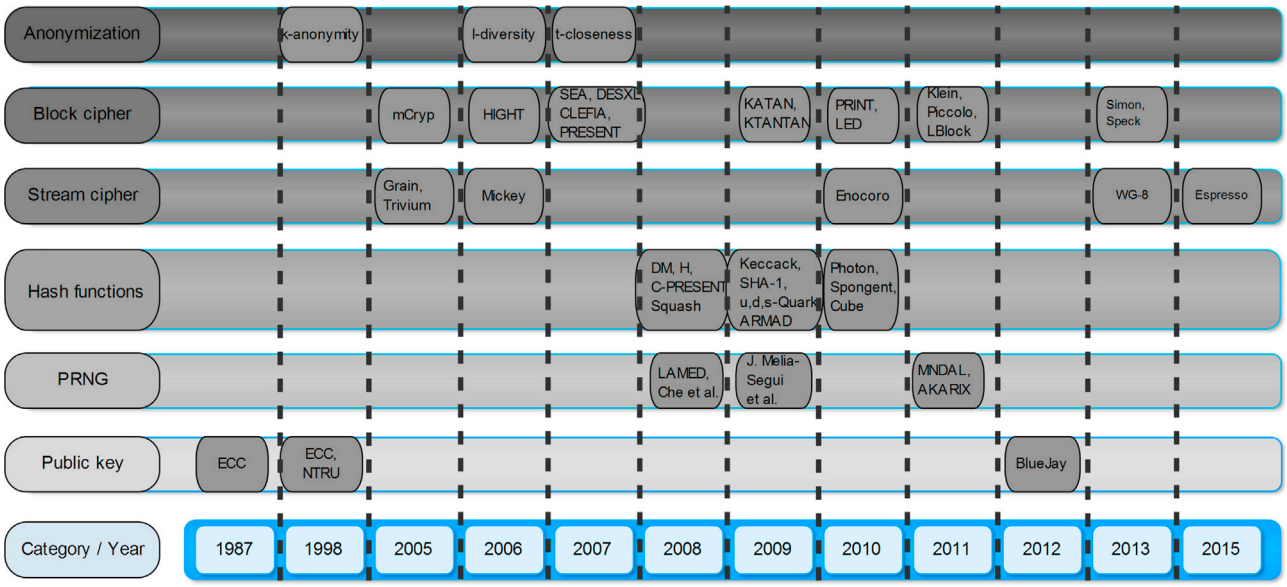


Fig. 4. Timeline of algorithms and research activities in IoT privacy.

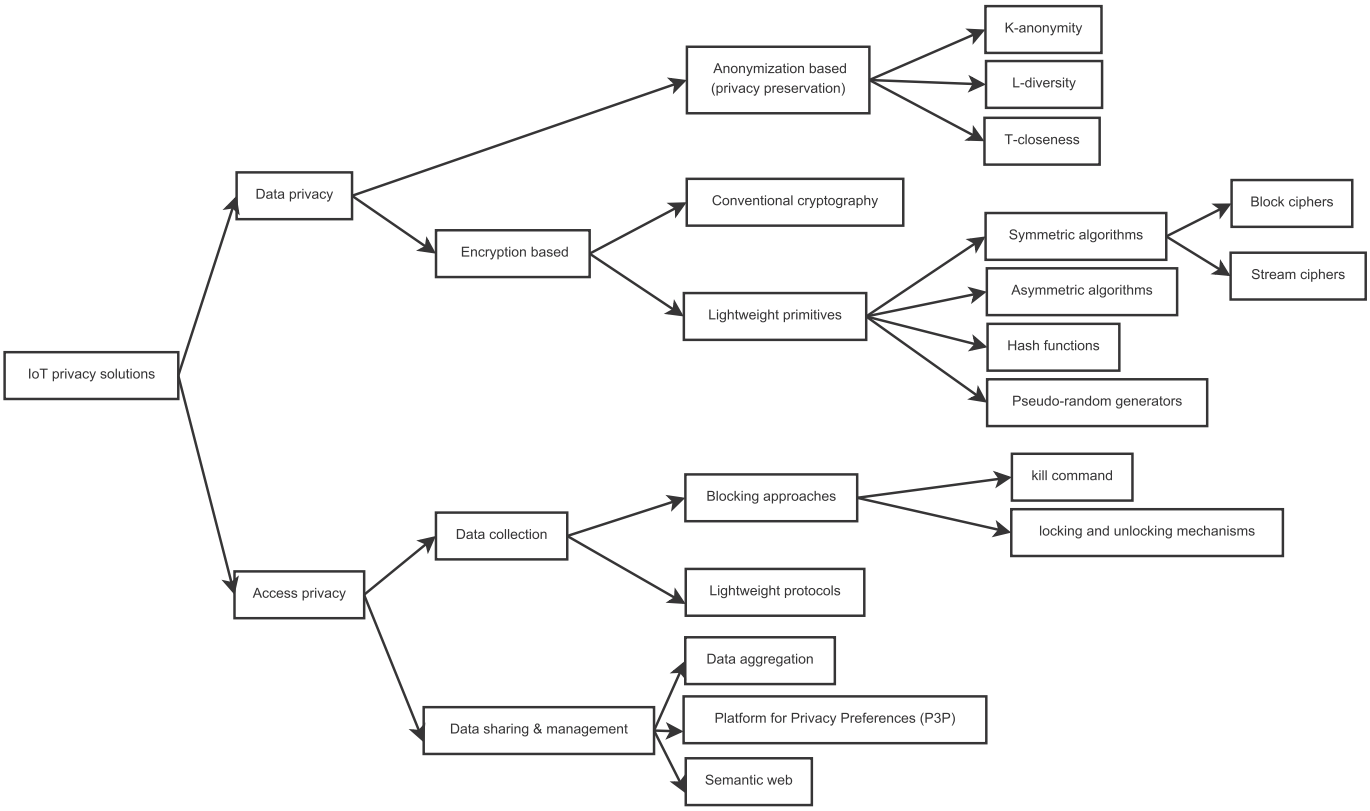


Fig. 5. Projects and research activities in data privacy.

problem of reducing the amount of significant information that may be extracted from the released data in the t-closeness case. In [31], a new proposal is presented based on the post randomization method (PRAM) for hiding discrete data, and on noise addition for other cases. In the IoT context, this proposal may be used in many cases such as those in which perturbative methods for privacy are considerable, or in location-based services [31].

5.1.2.2. Blocks ciphers. In resource-constrained environments, communication of intelligent objects must overcome specific restrictions of energy, performances and efficiency. In these scenarios, conventional cryptographic primitives are infeasible. A detailed survey appears in [32], where Abyaneh et al. presented the state-of-the-art of lightweight algorithms and protocols for RFID systems. Block cipher primitives constitute the most fundamental category of cryptographic algorithms. They transform a binary plain text of a fixed length into a cipher text of the same length using a symmetric key. To ensure communication security, lightweight block ciphers were introduced toward the end of the 1990s. Lightweight primitives are known to have the the block size of their input data chosen between 32 and 64 bits, the use of elementary operations like binary XOR and binary AND, and the simplicity of the key schedule [33].

Traditional cryptography schemes, such as 3-DES and AES, continue to be U.S. government standard ciphers for non-classified data. Recently, the National Institute of Standards and Technology confirmed this point of view in [34]. However, these ciphers do not fit the IoT scenario well due to their constrained resources in terms of energy and real time execution, as explained and experimentally proved in [35], through a comparison of the estimated energy of three different ciphers.

Numerous research activities occurred and led to plenty number block ciphers primitives for IoT, including mCRYPTON [36], HIGHT [37], SEA [38], DESXL [39], CLEFIA [40], PRESENT [41], KATAN, KTANTAN [42], PRINT Cipher [43], TEA/XTEA [43], Kasumi [44], LED [45], CLEFIA [40], KLEIN [46], Piccolo [47], LBlock [48], Simon and Speck [49], etc. A comprehensive survey of lightweight algorithms was presented in [33], where Cazorla et al. presented a broad comparison of all these algorithms in terms of operation and performance. Some block ciphers are compared in Table 2 regarding their key sizes, block sizes, consumed area measured in gate equivalents (GEs), and technology values (μm) [50–52].

5.1.2.3. Stream ciphers. Plain text is enciphered entirely with a pseudo-random key stream, generated with the same length of plain text. The

Table 2
Block ciphers algorithms comparison.

Algorithm	Key size [bits]	Block size [bits]	Area (GE)	Technology value [μm]
PRINTcipher	80	48	402	0.18
PRESENT	128	64	1570	0.18
DESXL	184	64	2168	0.18
HIGHT	128	64	3048	0.25
KATAN	80	64	1054	0.13
KTANTAN	80	64	684	0.13
LED	128	64	1265	0.18
KLEIN	64	64	1981	0.18
Piccolo	80	64	683	0.13
LBlock	80	64	1320	0.18

Comparison is based on key sizes, block sizes, consumed area measured in gate equivalents (GEs), and technology values (μm). GEs is a measurement unit used to specify complexity of digital electronic circuits independently from manufacturer and technology, and corresponds to a silicon area for a dedicated manufacturing technology. Technology value refers to the level of semiconductor process technology and expresses the size of the finished transistor and other components.

encryption operation consists of XORing the plain text and key stream. Although this category of cryptographic primitives represents an alternative for block cipher, its use is still limited due to the long initialization phase needed before first usage. This drawback makes them unusable in some communication protocols. However, their main advantage is the simplicity of the implementation in hardware and the ease of usage when the plain text size is unknown.

Contrary to block ciphers, the number of lightweight stream ciphers for constrained environments is limited. The most important systems include hardware-oriented algorithms of the eStream project, namely Grain [53], Trivium [54], and MICKEY 2.0 [55]. Newer algorithms include WG-8 [56], Espresso [57], and A2U2 [58]. Enocoro v.2 [59] can be listed as a pseudo-random number generator for use in a stream cipher. In Table 3 we report a quick comparison between some algorithms in terms of key size, consumed area (GEs), and technology values (μm) [60,52].

5.1.2.4. Hash functions. They are used for message integrity verification, digital signatures, and fingerprints. They fulfill the following requirements: (1) easy to compute, (2) collision resistant, (3) pre-image resistant (it should be difficult to calculate a message m, such that $h = hash(m)$); and (4) second pre-image resistant. In resource-constrained contexts, lightweight cryptographic hash functions are necessary to reduce hardware and energy consumption. According to their publication date, we can consider the following algorithms: DM-Present, H-Present, C-present [61], SQUASH [62], Keccak [63], SHA1 [64], D,U, S-Quark [65], Armadillo-C [66], Photon [67], Spongent [68], Cube [69] and GLUON [70]. Some of these functions are compared in Table 4 regarding to their output size (bits), area (GEs), and technologies (μm) [71].

5.1.2.5. Public key algorithms. They involve a public key and a private key, and ensure security services such as non-repudiation, integrity, authentication, confidentiality, and key exchange. Their main advantage is the non-requirement of any preceding secret's exchange between the parties. However, conventional public-key cryptography algorithms such as RSA demand high processing capabilities and long keys to ensure a good level of security. RSA remains inappropriate for constrained devices because they need to process large numbers and long keys to realize sufficient security. In addition, small computing devices will no longer be able to accommodate large keys since key generation, encryption and decryption operations demand high power consumption.

In IoT, alternative public-key cryptographic schemes with shorter keys may be used such as ECC (Elliptic Curve Cryptography), HECC (Hyper-Elliptic Curve Cryptography) [72], NTRU [73] (developed for RFID), and BlueJay [74]. ECC and HECC use an algebraic structure of elliptic curves over finite fields and offer enhanced security. Owing to their short keys, they constitute an interesting choice for embedded environments of the IoT framework [72]. NTRU is a public key algorithm based on polynomial algebra and consists of reducing polynomials with respect to two different moduli. This high speed algorithm, noted for its simplicity of computation is convenient for energy-constrained devices [73]. A recent ultra-lightweight algorithm was proposed in [74], and consists of a combination of symmetric encryption (Hummingbird-2), asymmetric encryption (Passerine), and authentication code. Designed for RFIDs and WSNs, this algorithm may be a suitable solution for IoT. A brief comparison between some algorithms in terms of area (GEs) and technologies (μm) is shown in Table 5 [52].

Table 3
Stream ciphers algorithms comparison.

Algorithm	Key size [bits]	Area (GE)	Technology value [μm]
A2U2	56	284	0.13
Grain v1	80	1294	0.13
Trivium	80	2599	0.13
Mickey	80	3188	0.13

Comparison is based on key sizes, consumed area measured in gate equivalents (GEs) and technology values (μm).

Table 4
Hash functions comparison.

Algorithm	Output size [bits]	Area (GE)	Technology value [μm]
DM-PRESENT-80	64	0.18	1600
PHOTON-80/20/16	80	0.18	865
H-PRESENT-128	128	0.18	2330
U-Quark	128	0.18	1379
Armadillo-2B	128	0.18	4353
S-Quark	224	0.18	2296
D-Quark	160	0.18	1702
Keccak-f [200]	64	0.13	2520
SPONGENT-128	128	0.13	1060
SPONGENT-224	224	0.13	1728
SHA-1	160	0.13	5527
Cube 32	512	0.13	5988

Comparison is based on output sizes, consumed area measured in gate equivalents (GEs) and technology values (μm).

Table 5
Asymmetric algorithms comparison.

Algorithm	Area (GE)	Technology value [μm]
BlueJay	<3000	0.18
NTRU	3000	0.18
ECC	8104	0.18
HECC	14,500	0.13

Comparison is based on consumed area measured in gate equivalents (GEs) and technology values (μm).

5.1.2.6. PRNG (Pseudo-Random Number Generators). PRNG are used to produce an unpredictable output sequence. Many solutions have been proposed to generate on-board pseudo-random numbers to secure RFID and WSN systems protocols. In [75], the authors proposed a 16-stages PRNG, a combination of an oscillator output and a linear feedback shift register. Limited by the use of a linear structure, this PRNG was attacked in [76]. To prevent this attack, the authors of [76] have designed a PRNG using multiple primitive polynomials instead of one in the LFSR. In [77], the authors proposed a PRNG compliant to EPC C1 Gen2 standard, named LAMED, suitable for low-cost RFID tags and providing both 32-bit and 16-bit random numbers. Other PRNGs were proposed in [78,79] and [80].

5.1.3. Access privacy

As shown in Fig. 6, techniques and research activities relating to the access privacy of data in the IoT include blocking approaches, lightweight protocols, data sharing and management.

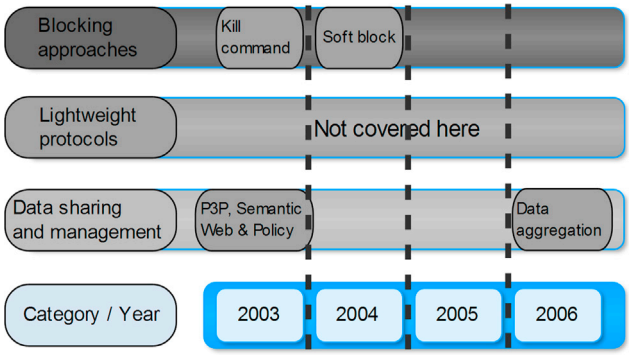


Fig. 6. Timeline of algorithms and research activities in access privacy.

5.1.3.1. Blocking approaches. During the phase of data collection, blocking techniques are used to prevent privacy problems. Frequently, the intelligent object is carried by a person, which may represent his/her unique identifier, and may be attacked to extract movement information. In this case, to reduce the privacy risks, users can use the kill command of RFID tags to force a disabling operation [81,82]. However, in the case of intelligent objects that need the tags to their functioning, this may not be possible. One possible solution is the use of a locking and unlocking mechanism for the tags. This is efficient for flexible privacy rules, where only a part of the data is classified as private, instead of "the all-or-nothing policy", used in the kill command [82–85].

5.1.3.2. Lightweight protocols. They aim essentially to ensure identification and authentication. Additional properties may be included such as delegation and restriction, proof of existence, and distance bounding [32]. These protocols are detailed in Section 5.3.

5.1.3.3. Data sharing and management. Many research efforts have been directed at data management and sharing in IoT context, and can be found in [86,87]. Regarding aggregation of data collected by sensors, an important work can be found in [88], where Sang et al. proposed a method for securing data aggregation to extend the network lifetime, guaranteeing reliable data collection from sensors, and addressing a solution for node failure and healing. In [89], Veltri et al. proposed a protocol for secure data aggregation at pre-determined or unpredictable time applied in both contexts of IoT and VANETs (Vehicular Ad hoc Networks).

5.1.4. Open research issues

The large number of protocols and schemes listed previously reflects the adequate efforts provided by researchers. However, we are still able to identify three main research axes in privacy field. First, with the huge amount of data exchanged between IoT actors, it is interesting to implement applications for the data minimization principle to reduce the amount of personal data collected and that need to be saved. Second, researchers can focus on standardization of security and privacy mechanisms in IoT, and comply with the requirements of the new schemes and algorithms. Third, new mechanisms should be developed to provide users with the possibility of managing their own privacy settings instead of expecting the IoT system to implement their requirements.

5.2. Trust

Establishing, negotiating, updating and revoking trust among entities in the IoT context is an essential task. The main difficulty to overcome is the engagement of unfamiliar and unpredictable entities implementation of the trust mechanism. Owing to their heterogeneous and irregular composition, it becomes necessary to define a different evaluation of trust for objects, humans, and services. To guarantee success in a trust negotiation operation, the credentials of involved parties must be exchanged and verified to allow mutual trust to be established. Contrary to classic schemes where trust is built in a centralized manner and prior trust relationships are established, managing trust in a dynamic and distributed environment is a very challenging research activity [90].

5.2.1. Definition

In the literature, many definitions of trust were proposed according to different taxonomies. Cho et al. [91] detailed the concept of trust in many disciplines, such as sociology, economics, philosophy, psychology, organizational management, autonomic computing, and communications and networking. They distinguished trust, trustworthiness and trust management, and presented a detailed survey of trust mechanisms in MANETs. The first definition of trust was proposed in [92], and focused on reliability trust. The authors stated that "Trust is the subjective probability by which an individual, A, expects that another individual, B, performs a given action on which its welfare depends". They involved two main concepts: dependency and degree of trust (probability). The main drawback of this definition is that trusting a person remains an insufficient reason to depend on him/her. A second definition was introduced in [93] about decision trust, and stipulates that "Trust is the extent to which one party is willing to depend on something or somebody in a given situation with a feeling of relative security, even though negative consequences are possible". This definition is based on four concepts: dependency, reliability, utility, and risk.

To highlight the role of trust in decision mechanisms, a set of practical procedures, tools, and rules have to be considered: trust management. In [94], the authors define this concept as follows: "Trust Management is an approach to making decisions about interacting with something or someone we do not completely know, establishing whether we should proceed with the interaction or not". It focuses on trust establishing, updating, and revoking through the study of security policies, credentials, and trust relationships.

5.2.2. State of the art and taxonomy

Depending on the mechanisms of establishing and evaluating trust between different nodes, two main categories of trust management systems can be defined: deterministic trust, and non-deterministic trust. Deterministic trust includes policy-based mechanisms and certificates systems. Non-deterministic trust includes recommendation based, reputation based systems, prediction based, and social network based systems. Policy based trust employs a series of policies to manage authorization and identify minimum trust levels. Certificate systems utilize public/private keys and digital signatures to decide whether to trust the signer or not. They use a third party to issue and manage certificates (CA: Certification Authority), which is trusted both by the certificate owner and by the party relying upon it. Recommendation based trust uses prior experiences to determine trust, and may use either explicit recommendation or transitive recommendation. Reputation based systems exploit consumer feedback to rate service provider. Prediction based trust is useful when there is no prior information, and involved entities are more likely to trust one another. Social network based trust builds trust communities, an environment where members can share their opinions, experiences, events, etc. without privacy and judgment problems.

Reputation based systems consider the global reputation of the entity and its experience while social-network based systems are founded on subjective concepts, such as friendship, honesty, social reputation or recommendation. In [95], Suryanarayana et al. presented the results of the first survey about trust management in peer-to-peer applications. They divide trust management techniques into three types: policy-based, reputation-based, and social network-based. They surveyed related technologies and approaches of nine different trust management systems based on eleven comparison parameters. The result of their survey is summarized in Fig. 7.

During the last decade, networks infrastructures and components have evolved to ensure flexible and on-demand services. Trust management concepts and techniques need to be adapted and many research activities have been devoted to this direction. In [91], Cho et al. surveyed trust management systems for Mobile Ad Hoc Networks. They used a new taxonomy, where they focus on the interactions between heterogeneous, social, information, and cognitive communication networks. They consider the limitations of these networks in terms of resource consumption and dynamic properties (topology, mobility, ubiquity, etc). In their survey, they define the following purposes to compare between different trust management systems: intrusion detection, authentication, access control, key management, and isolating misbehaving nodes.

Using a broader vision, Noor et al. in [96] proposed a survey of trust management systems for the cloud computing. They detail the principal techniques and research activities that may be adapted to services in cloud environments. They adopt a holistic vision of various trust management techniques where they define four categories: policy,

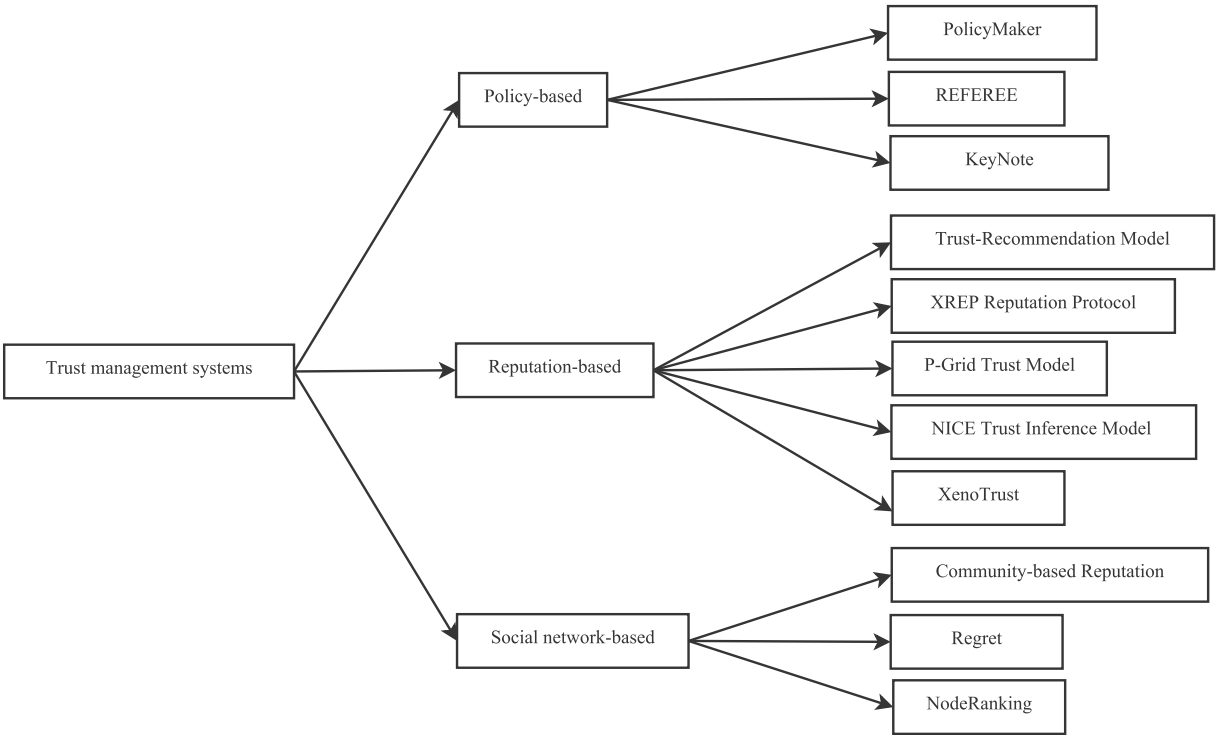


Fig. 7. Classification of trust management systems according to [95].

Table 6
Research activities related to trust management.

Trust category/ environment	Policy-based	Recommendation-based	Reputation-based	Prediction-based
P2P systems	[97]	[98–100]	[101–106]	[107,108]
GRID systems	[97]	[109]	[110–113]	[114–116]
Service oriented	[117, 118]	[119,120]	[119, 121–124]	[120,125]
Cloud environment	[126, 127]	[128,129]	[128–132]	[129,131, 132]
Web applications	[133]	[134]	–	[135]

recommendation, reputation, and prediction, as shown in Table 6. Depending on the trust applications, research activities are divided into fives classes as shown in Table 6: Peer to Peer (P2P) systems, GRID systems, a service-oriented environment, a cloud environment and web application.

Researchers made a considerable effort to adapt and propose new trust schemes to the severe constraints of dynamic networks. For example, the project uTRUSTit (Usable Trust in the Internet of Things),[8] applicable to the smart home/office environment and e-voting infrastructure, aims to develop a trust feedback toolkit and ameliorate a trust relationship between users. In this project, trust is defined differently: "A user's confidence is an entity's reliability, including acceptance of vulnerability in a potentially risky situation". The model of trust is based on a cognitive approach to define and fulfill user requirements and preferences. Trust is conceived as an internal status depending on users preferences, comprehension and experience including the reputation relationship.

In [136], Glior and Wing defined a model consisting of trust for heterogeneous networks consisting of humans and computers in which they combined both computational trust and behavioral trust concepts. They aimed to strengthen computational trust methods using behavioral trust to face the increased participation of humans in modern networks (social networks, online games, economical services, etc.). The reliability of the provided services should take into consideration the participation of the newly added users. The authors state that trust establishment must occur according to the user's preferences and beliefs, and demonstrate how behavioral trust is useful to establish a solid trust relationship between humans and computers.

In [137], Atzori et al. introduced a new paradigm for social network of intelligent objects based on a new paradigm of social relationships named Social IoT (SIoT). Similar to social networks for people, the authors define social network of intelligent objects, which refers to the social relationships between objects. Inspired by research activities about trust in P2P networks, the authors of [138] built a subjective model for trust management in SIoT. The basic rule for trust calculation is based on a node's experience and reputation among its common friends. To calculate the trust value, the authors developed a feedback system, where they merged the trustworthiness and centrality of the nodes involved.

5.2.3. *Open research issues*

As we notice the need for a general and generic theory for trust in heterogeneous networks where humans and objects need to interact, it is interesting to solve foundation limitations in this field. Furthermore, understanding the exact relationship between computational trust and behavioral trust in the IoT seems to be a worthy cause. Moreover updating the trust in changing network environments should be studied by researchers as the involved parties may be exposed to external attacks or may face severe energy conditions. Finally, although various mathematical models of trust were proposed, their applications in real networks remain limited. Conceiving and implementing trust mechanisms to protect services/users/objects in changing infrastructures is a good research direction. We believe that it is interesting to integrate trust within the access control scheme in these environments to build an efficient network.

[8] http://www.utrustit.eu.

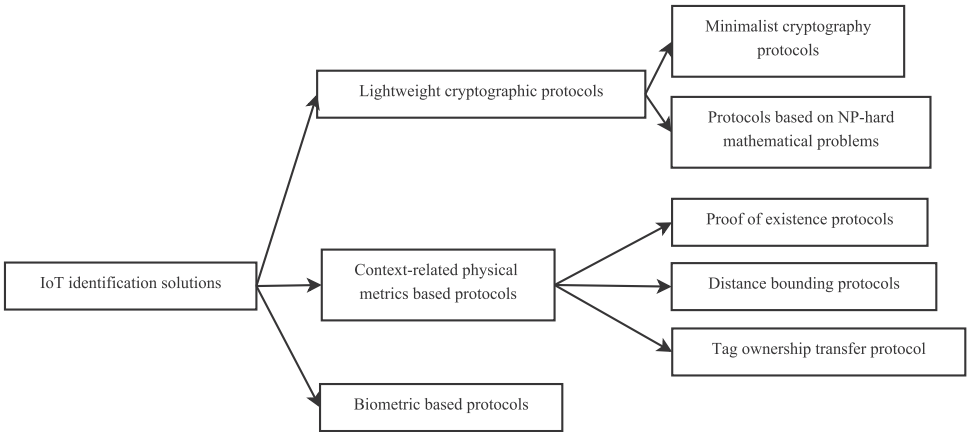


Fig. 8. Projects and research activities in identification – authentication.

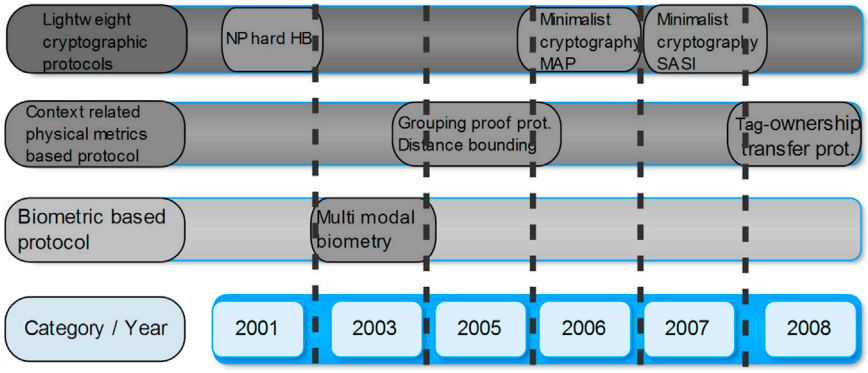


Fig. 9. Timeline of algorithms and research activities in identification – authentication.

5.3. Identification/authentication

5.3.1. Definition

Identification is used for devices, such as computers, servers, application gateways, RFID tags/readers, sensors, actuators, and more. They are associated with an identifier, such as RFID tag identifiers, an IP address, URIs (Universal Resource Identifier), or hostname, etc. More precisely, three categories of IoT identifiers can be differentiated: (1) Object Identifiers, used for physical or virtual objects, (2) Communication Identifiers, used to identify devices when they are communicating with other devices, and (3) Application Identifiers, used for applications and services [139]. Authentication is the process of confirming an entity's identity using a login and additional information to sign in, such as passwords, PIN, smart cards, digital certificates, and biometrics. It is used to prevent unauthorized access to resources.

5.3.2. State of the art and taxonomy

According to credential elements, research activities can be divided into three main groups, as shown in Figs. 8 and 9: (1) cryptographic primitives and ultra lightweight operations, (2) capabilities of EPCglobal Class-1 Generation 2; and (3) physical primitives [140]. Cryptographic primitives consist of hash functions (hash chain protocol, random hash-lock protocol) [141], MACs, PRNGs, stream ciphers, block ciphers, and public keys [142]. Ultra lightweight operations comprise simple binary functions such as XOR, AND, OR and rotations; or NP-hard mathematical problems. EPCglobal Class-1 Generation 2 capabilities intend to authenticate nodes using the 16-bit CRC and 16-bit RNG of the standard. Physical primitives utilize electronic and physical properties of RFID tags to form an authentication primitive [32].

5.3.3. Lightweight cryptographic protocols

The proliferation of tiny embedded networks produced the need to develop efficient cryptographic systems with limited resources consumption (energy, memory, processing). The arrival of IoT accentuates the problem of scarce resources by adding the scalability issue. Existing cryptographic algorithms necessitate processing, memory and energy capabilities, which may be unavailable in limited resources and embedded objects. The development of strong and cost-effective cryptography, combined with advanced energy producing techniques, constitutes an adequate solution to solve this problem. Many research efforts have shown that elliptic curve cryptography represents a strong security solution due to its limited resources consumption [143], and other researchers have demonstrated that energy may be generated from environmental conditions of interconnected objects (vibration, movement…) [144]. Lightweight cryptographic protocols can be divided into two groups: minimalist cryptography and protocols based on NP-hard mathematical problems. Minimalist cryptography includes Mutual Authentication Protocols (MAP) family (LMAP, EMAP, M2AP, etc.), and Strong Authentication and Strong Integrity (SASI) family. Protocols based on NP-hard mathematical problems contain Hopper and Blum (HB) family [32].

5.3.4. Context-related physical metrics based protocols

The ubiquity of IoT elements produces numerous interactions to distinguish information about their existence, exact position, precise timing and number/location of their neighbors. This category of protocols is based on the notion of physical primitives, which means the exploitation of electronic and physical properties of RFID tags to form an authentication primitive [32]. It includes three types of protocols: proof of existence, distance bounding and tag ownership transfer protocols.

Proof of existence protocols are known for two main families: Yoking/grouping proof protocols [145] and ECC-based grouping proof protocols [146]. In Yoking/grouping proof protocols (developed in 2004), the main goal is to unquestionably prove the physical presence of two or more RFID tags at the same location using information generated by one or more readers. This technique is based on random numbers generated by the tags separately [145]. In 2005, this proposal was generalized to grouping proofs using ECC cryptography to allow the participation of many tags in the proof generation [146].

Distance bounding protocols are used to prevent relay attacks, distance fraud, and terrorist attacks by monitoring the distance between any tag and its reader. This operation comprises a slow phase and a fast phase [147].

The tag ownership transfer protocol involves three entities: current/old owner, tag and new owner; and is executed in two phases: authentication and ownership transfer. Examples of this type of protocols contain those exploiting a Trusted Third Party (TTP) and decentralized proposals without TTP [148].

5.3.5. Biometric based protocols

The absence of physical security may lead to serious attacks, where malicious entities exploit compromised objects to retrieve sensitive data, and gain privileged access rights. Greenstadt et al. recommended the use of multi-modal biometrics to permit the object to identify its owner, and human-like security models to allow decision-making by the object [149]. In practice, biometric identification may include fingerprints, eye texture, voice, hand patterns, and facial recognition. The main goal is to realize sufficient natural recognition of the object's owner to avoid many threats and prevent security attacks

5.3.6. Open research issues

To contribute to identification development in IoT, the following research directions may be explored. First, it is important to address a global identification scheme to process a large number of object identification schemes. The hierarchical naming scheme used in the Internet is inadequate for dynamic environments, and industries utilize proprietary standards for identification, which aggravates the problem. Second, an infrastructure with non-colliding unique addresses should be set up. It is meaningful to take into account the random character of intelligent objects (arrival, departure from the network…), and allow the choice between disclosing or concealing their identities. In addition, to satisfy the interoperability requirements, it should be possible to recuperate information about a particular entity, with respect to its privacy preferences. Third, techniques of automatic discovery are useful to set up communications between humans and objects when the entities, services and network equipment, and topologies are continuously changing.

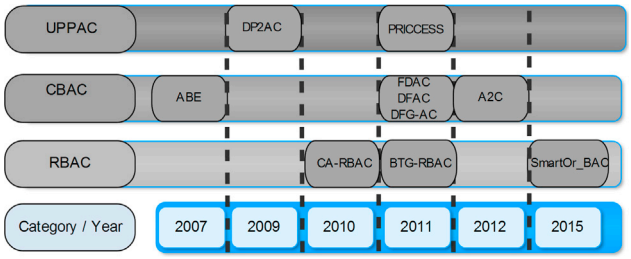


Fig. 11. Timeline of access control models.

5.4. Access control

5.4.1. Definition

Access control aims to manage the interaction and communication between users and systems. It attributes and checks authorizations to entities to execute precise operation(s) [150]. Traditionally, access control systems offer different specifying methods, which realize diverse degrees of granularity, flexibility, scope, and distinct categorizations of the controlled resources [151].

5.4.2. State of the art and taxonomy

In IoT, conventional ACLs are difficult to manage due to their complexity and lack of flexibility. They are replaced by other models as shown in Fig. 10. In [152], the authors survey access control models in WSNs. In Fig. 11, we classify research activities in access control systems in a two-dimensional diagram as described in [152].

In Role Based Access Control, the possible decisions are: permitted or denied access. For dynamic environments, many access control models where developed based on the RBAC approach to provide further security properties. Context-Aware Role-Based Access Control intends to ensure context awareness and adapt security parameters to ensure the users' security according to three modular context situations: critical, emergency, and normal condition [153]. Break-the-Glass Role-Based Access Control (BTG-RBAC) aims to collect information from end users to execute the BTG action in emergency situations. The system enquires whether the user really wants to perform emergency action, and consequently triggers alarms, the file, etc. [154]. In addition, the Organization Based Access Control (OrBAC) model is a generic and expressive access control model that extends the Role Based Access Control (RBAC) model. It expresses the security policy and enables distinction between an abstract policy defining organizational requirements and its real

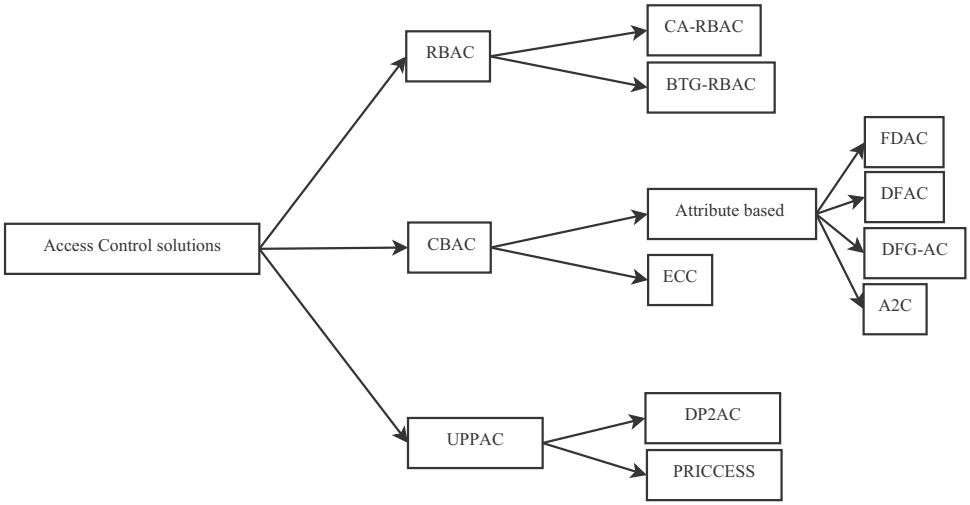


Fig. 10. Classification of access control systems [152].

implementation in a given information system. The SmartOrBAC model distributes processing costs between IoT devices with different levels of energy limitations and addresses the collaborative aspect with a specific solution [155].

Cryptography-Based Access Control (CBAC) is conceived for untrusted environments, and utilizes cryptography methods to control data access. It offers benefits in terms of distributed management, support for delegation, traceability of the access, authentication chains to extend scalability. Mainly, two different schemes may be used: ECC, and attribute-based encryption (ABE). In the latter scheme, four access control models may be distinguished: Fine-Grained Distributed Data Access Control (FDAC) [156], Distributed Fine-Grained Access Control (DFAC) [157], Distributed Fine-Grained Data Access Control for Distributed Sensor Networks (DFG-AC) [158], and Adaptive Access Control (A2C) [159].

Users' Privacy-Preserving Access Control (UPPAC) intends to hide the user's ID and protect private information. Hence, other network entities, with limited authorizations, become unable to know the actual users' ID

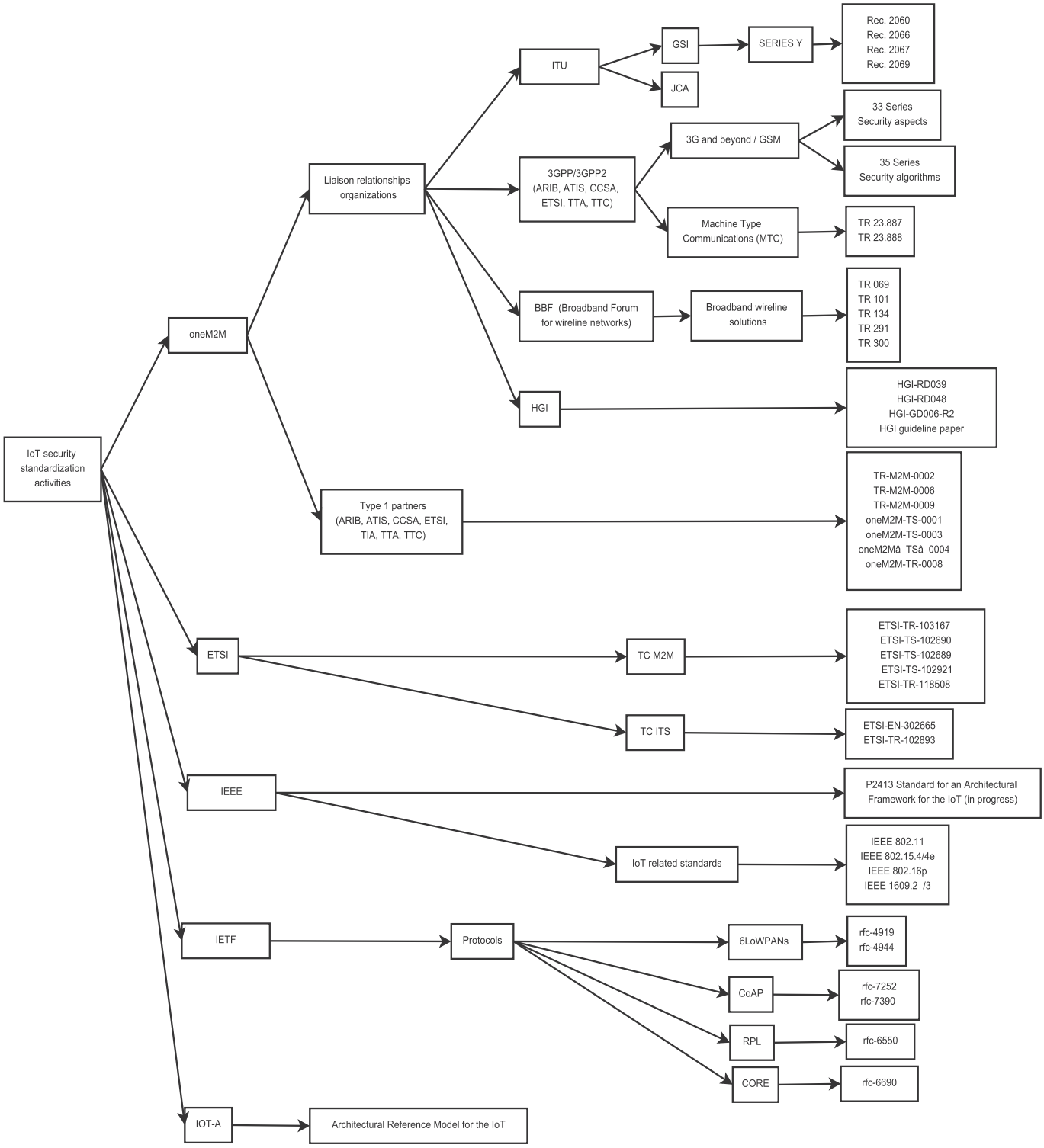


Fig. 12. Standardization in IoT.

[152]. In this context, we can distinguish two main access control models: Distributed Privacy-Preserving Access Control (DP2AC) [160], and PRICCESS [161].

5.4.3. Open research issues

Technical details provided in the previous sub-subsection lead to the definition of the following research axes in the access control field. First, credentials management is a crucial issue in the IoT context, especially regarding large amount of data which presents new implementation challenges. In [162], authors claim that interactions between objects and users, make credential management more challenging, and scalability concerns have to be debated. In addition, the multiplicity of identification schemes techniques imposes fine investigation to overcome technological difficulties.

Second, the ubiquitousness of interacting entities makes many operations possible, in the form of data sharing, entertainment, and resources distribution. This leads to higher cooperation between entities, and creates new sharing vector through mobility of communicating devices, which may constitute a major object for security attackers. Consequently, it is meaningful to build up successful solutions for secure sharing in IoT context, utilizing access control schemes, while supporting mobility feature.

6. Standardization activities in IoT security

Many industries are now engaged in IoT technologies due to the increasing number of inter-device communications. A single customer may target simultaneously products of different areas (health, smart grids, fitness, transportation, etc.). Then, manufacturers of IoT devices and applications need to handle unique security features that IoT components have to face once they are connected to each other. To fulfill this challenge, regulators and interoperability bodies must develop security standards to speed up IoT evolution and minimize costs as illustrated in Fig. 12. In this section we present the major actors of the standardization efforts for IoT security and their relevant activities.

6.1. Actors

The number of IoT security standardization bodies has increased in the last few years. They instituted considerable efforts leading to numerous standardization activities. The issued standards are either achieved by a single organization (ETSI, IEEE, IETF, etc.), or result from the collaboration among different organizations (oneM2M, IoT-A, etc.) as explained below.

6.1.1. OneM2M[9]

It is the global standards initiative for M2M communications and IoT. Many standardization organizations are assembled to generate many specifications for a common M2M Service Layer. The main results of oneM2M efforts activities are listed below.

6.1.2. ITU-IoTGSI (ITU-Global Standards Initiative on the Internet of Things)[10]

This initiative aims to unify research activities related to the IoT within ITU-T. It focuses on definitions, overviews, requirements, architecture, and a work plan for deploying the IoT. In this trend, ITU-T collaborated with other Standards Developing Organizations (SDOs) to publish many recommendations in the IoT field. This is valuable for service providers as it enables them to propose and improve services in this area. In practice, many recommendations were approved in the Y series, which is directed at the global information infrastructure, Internet protocol aspects and next-generation networks. More precisely, recommendations that are directly related to the IoT are Y.2060 (Overview of Internet of Things) and Y.2061 (Requirements for support of machine-oriented communication applications in the NGN environment) where a reference model of 4-layers is proposed for IoT architecture. Security questions are divided into two types: generic security capabilities and specific security capabilities. The former type of security capabilities is independent of applications and includes authorization, authentication, data confidentiality, integrity protection, privacy protection, security audit and anti-virus. Specific security capabilities depend on application requirements such as mobile payment.

6.1.3. 3GPP/3GPP2 (3rd Generation Partnership Project)[11]

It is a collaborative project between six SDOs (ARIB, ATIS, CCSA, ETSI, TTA, TTC), that are concentrated on developing technical reports and specifications for cellular technologies, such as 3.9G (LTE) and 4G (LTE-Advanced) and mobile network-based M2M. IoT standardization efforts within 3GPP/3GPP2 can be classified into two categories: mobile networks designed for human-to-human or human-to-machine interactions (GSM, 3G, 4G, etc.), and Machine-to-Machine interactions (also known as Machine Type Communications (MTC)). First, with the explosion of the number of connected devices, LTE (Long Term Evolution) seems to be the main connectivity technology in the IoT context. Here, the convergence of the IoT and 3GPP LTE network is of interest. This means that standard interfaces need to be defined to fulfill interoperability needs. A self-organizing network (SON) for LTE of 3GPP is a good proposal that other NGN standards should follow. Regarding security concerns, LTE applies specific security functions for data transmission. It focuses on signaling protection, user plane protection, network domain security, authentication and key agreement. The authentication procedure can be ensured either by the operator of the network, or by base stations in the case of mutual authentication or using authentication keys / digital certificates. Thus, considerable efforts were made to address security questions; 3GPP issued two technical specifications series, namely, the 33 series (Security aspects) and 35 series (Security algorithms). They include several documents defining various aspects of LTE security aspects, including architecture, Network Domain Security, IP network layer security, authentication Framework, Inter-Domain Trust Establishment, Application Security, and MVPN Access to Home. Second, 3GPP standardization activities on mobile network-based M2M are known as “Machine Type Communications (MTC)”. They focus on the optimization of access and core network infrastructure, permitting effective provision of M2M services. Many specifications covering use cases, service requirements, and a functional architecture for MTC application were released and approved. Further, 3GPP discussed secure telecommunication functions in MTC, including authorization, authentication, identification, access control, confidentiality and privacy. These features were debated in many Technical Reports such as TR 23.887 and 23.888.

6.1.4. BBF (BroadBand Forum)[12]

This forum has a large membership, including service providers, vendors, consultants, academic institutes, and test labs. Its main roles are related to engineering solutions to provide adequate broadband deployments. Within its M2M activities, BBF aims to enable, among others, services in the Smart Home to manage growing ecosystem of M2M/IoT. The forum launched an important initiative in network architectures with the release of a set of technical reports, and by defining its own TR-069 protocol suite and data models for home network management. It is worth mentioning that the TR-069 protocol is designed to function on secure transport protocols such as secure HTTP transport over TLS to ensure data confidentiality. Moreover, in its various TRs and TSs, the BBF discussed protection against MAC address spoofing and DoS attacks, protection against broadcast/multicast storms, ARP processing and IP

[9] http://www.onem2m.org.
[10] http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx.
[11] http://www.3gpp.org/.
[12] http://www.broadband-forum.org.

spoofing prevention to avoid malicious attackers.

6.1.5. HGI (Home Gateway Initiative)[13]

This initiative aims to develop a smart home ecosystem, and publish requirements and test plans for home gateways and wireless/wireline home networks. It improves applications, and facilitates connections of home gateway middleware and communicating devices. The HGI issued technical requirements for devices and services in the smart home including gateways and networks. It published technical requirements for home gateways including QoS, and software modularity. In the security area, HGI discussed many aspects, including security management procedures, firewall policy, key management, WLAN security and authentication mechanisms. In practice, many specifications were interested in the aforementioned security questions such as the HGI Guideline Paper, HGI-RD048 (HG requirements for HGI open platform 2.0) and HGI-GD006-R2 (HGI guideline paper IMS Enabled HG).

6.1.6. Type 1 partners technical specifications and technical reports

OneM2M has established two types of partners: type 1 and type 2. The second type involves a limited number of organizations and plays a key role in the dissemination of standards. The first type includes many Standards Development Organizations (SDO) and plays an important role in technical specifications and technical reports publishing. In IoT context, many efforts were provided within M2M communication and oneM2M framework to propose a general framework, technical requirements and security requirements for IoT. Also, a special interest was given to semantic web best practices where guidelines for domain knowledge interoperability to build the Semantic Web of Things were proposed. In security context, considerable contribution can be noticed regarding security and privacy aspects, including authentication, encryption and integrity verification. More details are related to authorization, access control, confidentiality, authentication, identification, trust and integrity verification can be found in oneM2M-TS-0003 (oneM2M Security Solutions) and oneM2M-TR-0008 (oneM2M-TR-0008-Security).

6.1.7. ETSI (European Telecommunications Standards Institute)[14]

This institute comprises two main technical committees: ETSI M2M and ETSI ITS (Intelligent Transport Systems). ETSI M2M focuses on the services, functional requirements, interfaces and architecture of M2M solutions, divided into five domains, namely: smart grids, health, connected consumers, transportation, and smart cities. Security aspects debated by ETSI M2M technical committee are related to authentication, integrity, confidentiality, trust management and access control (e.g. TS-102690, TR-118-508). ETSI ITS debates all types of vehicular communications. In security context, ETSI ITS discusses confidentiality, integrity, availability, accountability and authenticity (e.g. TR-102-893).

6.1.8. IEEE (Institute of Electrical and Electronics Engineers)[15]

The institute involves the P-2413 standardization project, which aims to build an architectural framework for the IoT. The standard intends to supply a quadruple trust feature (protection, security, privacy, and safety). Besides, IEEE contributed to Smart Grid (SG) field development, and issued important related standards (e.g., IEEE-2030, IEEE 1711 and IEEE 1686-2007) where different security features are discussed, including specific serial security, safeguards, audit mechanisms, access control, data recovery, etc. Besides, we can list many other standards issued by IEEE, not directly linked to IoT but can be used or adapted to answer its requirements, such as IEEE-802.15.4 (ZigBee) and IEEE 802.16p (IEEE Standard for Air Interface for Broadband Wireless Access Systems). The first example is known as a Low Rate Personal Area Network and includes a set of security functions located at the datalink level, namely, access control, integrity verification, data confidentiality and protection against replay attacks. The second example aims to enhance the support of M2M applications through the management of information exchange between a subscriber station and a server in the core network (through a base station) or between subscriber station without any human interaction. The security of this standard lies in supporting the integrity and authentication of M2M devices; integrity and privacy of M2M application traffic; device validity check; and enabling a flexible security suite to meet the requirements of the M2M application.

6.1.9. IETF (Internet Engineering Task Force)[16]

This tasks force is interested in the semantic web, social networks and RESTful services. First, it contributed to the IPv6 supported by limited-energy devices in 6LowWPAN-IPv6 protocol (IPv6 over Low-Power Wireless Personal Area Networks). This protocol adopts the same security features as IEEE 802.15.4 and IPv6. Second, IEEE issued the Constrained Application Protocol (CoAP) for resource-constrained devices to facilitate translation to HTTP for integration purposes with web application. Regarding security aspects, this protocol discusses authentication, integrity, confidentiality and protection against replay attacks. Third, IETF developed the PRL (IPv6 Routing Protocol for Low-Power and Lossy Networks) protocol in RFC6550. The security of this protocol adopts three modes (unsecured mode, pre-installed mode and authenticated mode). Fourth, IETF proposed an integrated web services for M2M and IoT applications, named CoRE (Constrained RESTful Environment) which applies the same security features as HTTP over TLS (RFC2818).

6.1.10. IoT-A (Internet of Things – Architecture)[17]

It proposes an architectural reference model for the IoT context, made up of a suite of key building blocks. The main objective is to assist providers and researchers when they have to make their technical choices. Thus, IoT-A provides design directives with simulation and prototyping options. Many security features are deeply debated in this model and are related to authorization, authentication, identification, key management, and trust management.

6.2. Open research issues

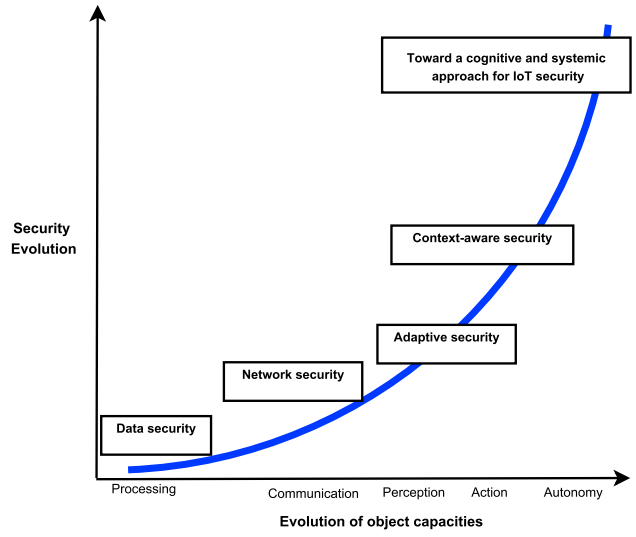
Although considerable research has been devoted to the IoT security domain, we can still propose many issues that need to be addressed. First, the security of IoT endpoints is crucial since we are concerned with a huge number of intelligent objects. Then, efficient authentication standards need to be proposed and have to take into consideration names unifying, encoding, profiles and privileges, an explicit trust relationship, a time-tamping protocol, etc. Second, a considerable interest should be paid to IoT ecosystems. A huge data ecosystem registry is needed to facilitate the tracking of all parties that may affect the security of IoT system components during their life-cycle. Finally, IoT interactions need to be debated among IoT security concerns. A security incident and event management repository would be useful to study IoT logs for predictive, real-time, and historical analyses.

7. Discussion

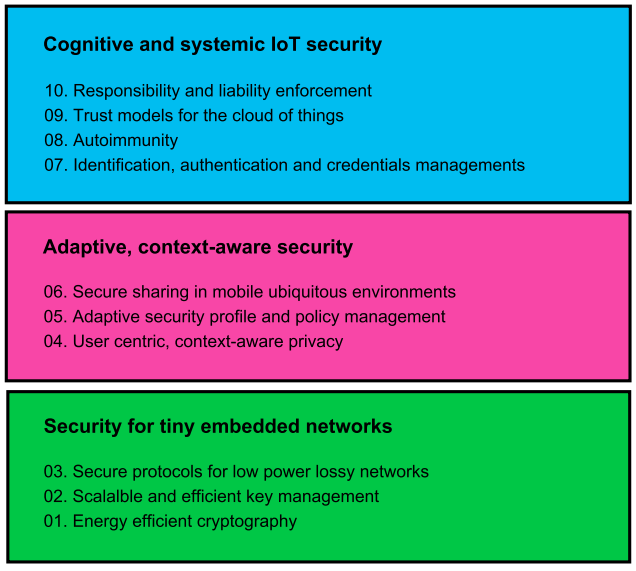
IoT enables objects to become active participants. They become able to recognize events and changes in their environment, and react more or less autonomously without human intervention. Computer networks, instead of simply being networks of calculators that process data, are expected to become intelligent networks capable of sensing, perceiving and recognizing, acting and reacting, and will continue to evolve to become more autonomous.

As illustrated in Fig. 13, in parallel with the increasing autonomy of

[13] http://www.homegatewayinitiative.org/.
[14] http://www.etsi.org.
[15] http://www.ieee.org.
[16] http://www.ietf.org.
[17] http://www.iot-a.eu.



(a) Evolution of security requirements



(b) Research axes for IoT security and privacy

Fig. 13. Evolution of security requirements and research axes for IoT security and privacy.

objects to perceive and act on the environment, IoT security should move towards a greater autonomy in perceiving threats and reacting to attacks, based on a cognitive, systemic approach. We summarize three IoT security research axes: efficient security for tiny embedded networks, adaptive, context-aware and user-centric security, and a cognitive, systemic approach to securing the IoT.

An urgent prerequisite for securing IoT is the development of *efficient security mechanisms for tiny embedded networks* with scarce resources. Current developments in wireless sensor and actuator networks, RFID technology, mobile computing and so forth, demonstrate the resource scarcity of the devices and technologies that will be part of the IoT. Consequently, much research work is being devoted to developing efficient, robust and low-consumption cryptography for tiny embedded computing and secure protocols for low-power lossy networks. It is essential to adapt and/or design related and equally important subsystems, such as key management, authentication mechanisms, credential management, and so on.

The ubiquitous nature of IoT raises legitimate questions about the privacy of persons, and how to cope with the heterogeneity of user and application requirements in terms of security services. This requires the development of *adaptive, context-aware and user-centric security solutions*. This diversity in terms of security requirements can be addressed via the adaptive, context-aware management of security profiles and policies. The ubiquity of objects encourages content sharing which, in turn, means paying special attention to security and privacy in a dynamic and heterogeneous environment.

Similar to objects being autonomous to perceive and act on their environment, IoT security should evolve towards greater autonomy in detecting threats and reacting to attacks by following a *cognitive, systemic approach*. This evolution relates to the autoimmunity of intelligent objects so as to prevent and contain attacks in a potentially hostile environment. Adequate trust models will be required to guarantee the smooth and peaceful evolution of objects in a large, heterogeneous technological ecosystem. Autonomous object actions require responsibility management and liability enforcement when detecting threats and reacting to attacks. Finally, most attacks can be prevented through a strong identification and recognition of object owners.

8. Conclusion

The IoT is a new disruptive technology that can be expected to bring about an evolution in usage and in the surrounding technological ecosystem. In this paper, we have shown that this major evolution creates its own security and privacy challenges. Most of these challenges result from the inherent vulnerabilities of IoT objects and the tight coupling of the physical world to the virtual world through intelligent objects. This tight interaction highlights a systemic dimension of IoT security that we proposed to use as a roadmap overview in this work. We then surveyed security related interactions and solutions: Privacy, Trust, Identification and Access Control. In addition to highlighting scientific and technological locks we have shed light on the main standardization activities and the open issues. We also showed that the evolution of objects towards greater autonomy intensifies the issues of security and privacy. Finally, we concluded that the autonomy of objects to perceive and act on their environment would cause IoT security to move towards greater perceptive and actionable autonomy based on a cognitive and systemic approach.

References

[1] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of things (Iot): a vision, architectural elements, and future directions, Future Gener. Comput. Syst. 29 (7) (2013) 1645–1660.
[2] H. Sundmaeker, P. Guillemin, P. Friess, S. Woelffle (Eds.), Vision and Challenges for Realising the Internet of Things, 2010.
[3] B. Zhu, A. Joseph, S. Sastry, A taxonomy of cyber attacks on scada systems, in: Proceedings of the 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing, ITHINGSCPSCOM'11, IEEE Computer Society, Washington, D.C., USA, 2011, pp. 380–388.
[4] Y. Challal, Securite de l'internet des objets: vers une approche cognitive et systemique, Hdr, Universite de Technologie de Compiegne, 2012.
[5] A. Riahi, Y. Challal, E. Natalizio, Z. Chtourou, A. Bouabdallah, A systemic approach for iot security, in: Proceedings of the DCOSS, IEEE, 2013, pp. 351–355.
[6] L. Atzori, A. Iera, G. Morabito, The internet of things: a survey, Comput. Netw. 54 (15) (2010) 2787–2805.
[7] D. Miorandi, S. Sicari, F. de Pellegrini, I. Chlamtac, Survey internet of things: vision, applications and research challenges, Ad Hoc Netw. 10 (7) (2012) 1497–1516.
[8] C.C. Aggarwal, N. Ashish, A.P. Sheth, The internet of things: a survey from the data-centric perspective, in: C.C. Aggarwal (Ed.), Managing and Mining Sensor Data, Springer US, Boston, MA, 2013, pp. 383–428.
[9] O. Said, Accurate performance evaluation of internet multicast architectures: hierarchical and fully distributed vs. service-centric, TIIS 7 (9) (2013) 2194–2212.
[10] C. Perera, A.B. Zaslavsky, P. Christen, D. Georgakopoulos, Context Aware Computing for the Internet of Things: A Survey, CoRR abs/1305.0982.
[11] O. Vermesan, P. Friess, P. Guillemin, S. Gusmeroli, H. Sundmaeker, A. Bassi, I.S. Jubert, M. Mazura, M. Harrison, M. Eisenhauer, P. Doody, Internet of Things Strategic Research Roadmap, Tech. Rep., IERC Cluster SRA, 2011.

[12] J. Granjal, E. Monteiro, J. Silva, Security for the internet of things: a survey of existing protocols and open research issues, IEEE Commun. Surv. Tutor. 99 (2015) 1.

[13] S. Sicari, A. Rizzardi, L.A. Grieco, A. Coen-Porisini, Security, privacy and trust in internet of things: the road ahead, Comput. Netw. 76 (2015) 146–164.

[14] J. Pescatore, G. Shpantzer, Securing the Internet of Things Survey, InfoSec Reading Room.

[15] D. Gil, A. Ferrandez, H. Mora-Mora, J. Peral, Internet of things: a review of surveys based on context aware intelligent services, Sensors 16 (7) (2016) 1069, https://doi.org/10.3390/s16071069. ⟨http://www.mdpi.com/1424-8220/16/7/1069⟩.

[16] A. Riahi, E. Natalizio, Y. Challal, N. Mitton, A. Iera, A systemic and cognitive approach for IoT security, in: Proceedings of the International Conference on Computing, Networking and Communications (ICNC 2014), Honolulu, United States, 2014, Invited Paper.

[17] L. Kiely, T.V. Benzel, Systemic security management, IEEE Secur. Priv. 4 (6) (2006) 74–77.

[18] R. Publishers (Ed.), Principles of Inductive Near Field Communications for Internet of Things, 2011.

[19] C. Liu, Y. Zhang, Z. Cai, J. Yang, L. Peng, Artificial immunity-based security response model for the internet of things, JCP 8 (12) (2013) 3111–3118.

[20] C. Liu, J. Yang, R. Chen, Y. Zhang, J. Zeng, Research on immunity-based intrusion detection technology for the internet of things., in: Y. Ding, H. Wang, N. Xiong, K. Hao, L. Wang (Eds.), Proceedings of the ICNC, IEEE, 2011, pp. 212–216.

[21] J. Pescatore, Securing the Internet of Things Survey: A Sans Analyst Survey, Tech. Rep., SANS Institute, January 2014.

[22] S. Yu, M. Liu, W. Dou, X. Liu, S. Zhou, Networking for big data: a survey, IEEE Commun. Surv. Tutor. 19 (1) (2017) 531–549, https://doi.org/10.1109/COMST.2016.2610963.

[23] S. Yu, Big privacy: challenges and opportunities of privacy study in the age of big data, IEEE Access 4 (2016) 2751–2763, https://doi.org/10.1109/ACCESS.2016.2577036.

[24] P. Samarati, L. Sweeney, Generalizing data to provide anonymity when disclosing information, in: Proceedings of the 17th ACM SIGACT-SIGMOD-SIGART Symposium on Principles of Database Systems (PODS 1998), Seattle, WA, USA, 1998.

[25] P. Samarati, Protecting respondents identities in microdata release, IEEE Trans. Knowl. Data Eng. 13 (6) (2001) 1010–1027, https://doi.org/10.1109/69.971193.

[26] W. Liu, B. Fang, L. Yin, X. Yu, A tree based location privacy approach against multi-precision continuous attacks in the internet of things, J. Inf. Comput. Sci. 9 (7) (2012) 1807–1819.

[27] Y. Xu, X. Qin, Z. Yang, Y. Yang, C. Huang, An algorithm of k-anonymity for data releasing based on fine-grained generalization, J. Inf. Comput. Sci. 9 (11) (2012) 3071–3080.

[28] A. Machanavajjhala, D. Kifer, J. Gehrke, M. Venkitasubramaniam, L-diversity: privacy beyond k-anonymity, in: Proceedings of the ACM Transactions on Knowledge Discovery from Data TKDD, 1(1), 2007, p. 146.

[29] N. Li, T. Li, S. Venkatasubramanian, t-C loseness: privacy beyond k-anonymity and l-diversity, in: Proceedings of the 23rd International Conference on Data Engineering (ICDE 2007), IEEE, 2007, pp. 106–115.

[30] M.V.R. NarasimhaRao, J.S. VenuGopalkrisna, R.V. Murthy, C.R. Ramesh, Closeness: privacy measure for data publishing using multiple sensitive attributes, Int. J. Eng. Sci. Adv. Technol. 2 (2) (2012) 278–284.

[31] D. Rebollo-Monedero, J. Forn, J. Domingo-Ferrer, From t-closeness-like privacy to postrandomization via information theory, IEEE Trans. Knowl. Data Eng. 22 (11) (2010) 1623–1636.

[32] M.R.S. Abyaneh, Security analysis of lightweight schemes for rfid systems, Tech. Rep., Dissertation for the Degree of Philosophiae Doctor, University of Bergen Norway, 2012.

[33] M. Cazorla, K. Marquet, M. Minier, Survey and benchmark of lightweight block ciphers for wireless sensor networks, in: P. Samarati (Ed.), Proceedings of the SECRYPT, SciTePress, 2013, pp. 543–548.

[34] K.A. McKay, L. Bassham, M.S. Turan, N. Mouha, Report on Lightweight Cryptography, draft nistir 8114, Tech. Rep., National Institute of Standards and Technology, August 2016.

[35] D. Kim, J.-Y. Choi, J.-E. Hong, Evaluating energy efficiency of internet of things software architecture based on reusable software components, Int. J. Distrib. Sens. Netw. 13 (1) (2017), https://doi.org/10.1177/1550147716682738.

[36] C.H. Lim, T. Korkishko, Mcrypton – a lightweight block cipher for security of low-cost rfid tags and sensors, in: J. Song, T. Kwon, M. Yung (Eds.), Proceedings of the WISA, Vol. 3786 of Lecture Notes in Computer Science, Springer, 2005, pp. 243–258.

[37] D. Hong, J. Sung, S. Hong, J. Lim, S. Lee, B. Koo, C. Lee, D. Chang, J. Lee, K. Jeong, H. Kim, J. Kim, S. Chee, Hight: a new block cipher suitable for low-resource device, in: L. Goubin, M. Matsui (Eds.), Proceedings of the 8th International Workshop on Cryptographic Hardware and Embedded Systems – CHES 2006, Yokohama, Japan, October 10–13, 2006, Vol. 4249 of Lecture Notes in Computer Science, Springer, 2006, pp. 46–59.

[38] F. Mace, F.-X. Standaert, J.-J. Quisquater, Asic implementations of the block cipher sea for constrained applications, in: Proceedings of the Third International Conference on RFID Security – RFIDSec 2007, 2007, pp. 103–114.

[39] G. Leander, C. Paar, A. Poschmann, K. Schramm, New lightweight des variants, in: A. Biryukov (Ed.), Proceedings of the FSE, Vol. 4593 of Lecture Notes in Computer Science, Springer, 2007, pp. 196–210.

[40] T. Shirai, K. Shibutani, T. Akishita, S. Moriai, T. Iwata, The 128-bit blockcipher clefia (extended abstract), in: A. Biryukov (Ed.), Proceedings of the FSE, Vol. 4593 of Lecture Notes in Computer Science, Springer, 2007, pp. 181–195.

[41] A. Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, M.J.B. Robshaw, Y. Seurin, C. Vikkelsoe, Present: an ultra-lightweight block cipher, in: P. Paillier, I. Verbauwhede (Eds.), Proceedings of the CHES, Vol. 4727 of Lecture Notes in Computer Science, Springer, 2007, pp. 450–466.

[42] C.D. Cannire, O. Dunkelman, M. Knezevic, Katan and ktantan – a family of small and efficient hardware-oriented block ciphers, in: C. Clavier, K. Gaj (Eds.), Proceedings of the CHES, Vol. 5747 of Lecture Notes in Computer Science, Springer, 2009, pp. 272–288.

[43] G.N. Khan, J. Yu, F. Yuan, Xtea based secure authentication protocol for rfid systems, in: H. Wang, J. Li, G.N. Rouskas, X. Zhou (Eds.), Proceedings of the ICCCN, IEEE, 2011, pp. 1–6.

[44] 3rd Generation Partnership Project, Specification of the 3GPP Confidentiality and Integrity Algorithms – Document 2: KASUMI Specification (Release 6), Tech. Rep. 3GPP TS 35.202 V6.1.0 (2005–09), 2005.

[45] J. Guo, T. Peyrin, A. Poschmann, M.J.B. Robshaw, The led block cipher, in: B. Preneel, T. Takagi (Eds.), Proceedings of the CHES, Vol. 6917 of Lecture Notes in Computer Science, Springer, 2011, pp. 326–341.

[46] Z. Gong, S. Nikova, Y.W. Law, Klein: a new family of lightweight block ciphers, in: A. Juels, C. Paar (Eds.), Proceedings of the RFIDSec, Vol. 7055 of Lecture Notes in Computer Science, Springer, 2011, pp. 1–18.

[47] K. Shibutani, T. Isobe, H. Hiwatari, A. Mitsuda, T. Akishita, T. Shirai, Piccolo: an ultra-lightweight blockcipher, in: B. Preneel, T. Takagi (Eds.), Proceedings of the CHES, Vol. 6917 of Lecture Notes in Computer Science, Springer, 2011, pp. 342–357.

[48] W. Wu, L. Zhang, Lblock: a lightweight block cipher, in: J. Lopez, G. Tsudik (Eds.), ACNS, Vol. 6715 of Lecture Notes in Computer Science, 2011, pp. 327–344.

[49] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, L. Wingers, Simon and speck: block ciphers for the internet of things, Cryptology ePrint Archive, Report 2015/585, 2015. ⟨http://eprint.iacr.org/2015/585⟩.

[50] Q. Chai, G. Gong, A cryptanalysis of hummingbird-2: the differential sequence analysis, IACR Cryptology ePrint Archive 2012, 2012, p. 233.

[51] D. Lee, D.-C. Kim, D. Kwon, H. Kim, Efficient hardware implementation of the lightweight block encryption algorithm lea, Sensors 14 (1) (2014) 975–994, https://doi.org/10.3390/s140100975. ⟨http://www.mdpi.com/1424-8220/14/1/975⟩.

[52] A.K. Manjulata, Survey on lightweight primitives and protocols for rfid in wireless sensor networks, Int. J. Commun. Netw. Inf. Secur. 6 (1) (2014) 29–43.

[53] M. Hell, T. Johansson, W. Meier, Grain: a stream cipher for constrained environments, Int. J. Wirel. Mob. Comput. 2 (1) (2007) 86–93.

[54] C.D. Canniere, B. Preneel, Trivium Specifications, eSTREAM, ECRYPT Stream Cipher Project.

[55] P. Kitsos, N. Sklavos, M. Parousi, A.N. Skodras, A comparative study of hardware architectures for lightweight block ciphers, Comput. Electr. Eng. 38 (1) (2012) 148–160.

[56] X. Fan, K. Mandal, G. Gong, WG-8: A Lightweight Stream Cipher for Resource-Constrained Smart Devices, Springer Berlin Heidelberg, Berlin, Heidelberg, 2013, pp. 617–632.

[57] E. Dubrova, M. Hell, Espresso: a stream cipher for 5g wireless communication systems, Cryptogr. Commun. (2015) 1–17, https://doi.org/10.1007/s12095-015-0173-2.

[58] M. David, D.C. Ranasinghe, T. Larsen, A2u2: a stream cipher for printed electronics rfid tags, in: Proceedings of the IEEE International Conference on RFID (IEEE RFID 2011), Orlando, Florida, USA, 2011.

[59] D. Watanabe, T. Owada, K. Okamoto, Y. Igarashi, T. Kaneko, Update on enocoro stream cipher, in: Proceedings of the ISITA, IEEE, 2010, pp. 778–783.

[60] C. Manifavas, G. Hatzivasilis, K. Fysarakis, K. Rantos, Lightweight cryptography for embedded systems – a comparative analysis, in: Proceedings of the DPM/SETOP, 2013, pp. 333–349.

[61] A. Bogdanov, G. Leander, C. Paar, A. Poschmann, M.J.B. Robshaw, Y. Seurin, Hash functions and rfid tags: Mind the gap, in: E. Oswald, P. Rohatgi (Eds.), Proceedings of the CHES, Vol. 5154 of Lecture Notes in Computer Science, Springer, 2008, pp. 283–299.

[62] A. Shamir, Squash – a new mac with provable security properties for highly constrained devices such as rfid tags, in: K. Nyberg (Ed.), Proceedings of the FSE, Vol. 5086 of Lecture Notes in Computer Science, Springer, 2008, pp. 144–157.

[63] E.B. Kavun, T. Yalin, A lightweight implementation of keccak hash function for radio-frequency identification applications, in: S.B.O. Yalcin (Ed.), Proceedings of the RFIDSec, Vol. 6370 of Lecture Notes in Computer Science, Springer, 2010, pp. 258–269.

[64] M. O'Neill, M.J.B. Robshaw, Low-cost digital signature architecture suitable for radio frequency identification tags, IET Comput. Digit. Tech. 4 (1) (2010) 14–26.

[65] J.-P. Aumasson, L. Henzen, W. Meier, M. Naya-Plasencia, Quark: a lightweight hash, in: S. Mangard, F.-X. Standaert (Eds.), Proceedings of the CHES, Vol. 6225 of Lecture Notes in Computer Science, Springer, 2010, pp. 1–15.

[66] S. Badel, N. Dagtekin, J. Nakahara, K. Ouafi, N. Reffe, P. Sepehrdad, P. Susil, S. Vaudenay, Armadillo: A multi-purpose cryptographic primitive dedicated to hardware, in: Proceedings of the CHES, 2010, pp. 398–412.

[67] J. Guo, T. Peyrin, A. Poschmann, The photon family of lightweight hash functions, in: P. Rogaway (Ed.), Proceedings of the CRYPTO, Vol. 6841 of Lecture Notes in Computer Science, Springer, 2011, pp. 222–239.

[68] A. Bogdanov, M. Knezevic, G. Leander, D. Toz, K. Varici, I. Verbauwhede, spongent: A lightweight hash function, in: B. Preneel, T. Takagi (Eds.), Proceedings of the CHES, Vol. 6917 of Lecture Notes in Computer Science, Springer, 2011, pp. 312–325.

[69] D. Bernstein, Cubehash: A Simple Hash Function. ⟨http://cubehash.cr.yp.to/⟩.

[70] T.P. Berger, J. D'Hayer, K. Marquet, M. Minier, G. T. 0002, The gluon family: A lightweight hash function family based on fcsrs, in: A. Mitrokotsa, S. Vaudenay (Eds.), Proceedings of the AFRICACRYPT, Vol. 7374 of Lecture Notes in Computer Science, Springer, 2012, pp. 306–323.

[71] X. Guo, P. Schaumont, The technology dependence of lightweight hash implementation cost, in: Proceedings of the ECRYPT Workshop on Lightweight Cryptography (LC2011), 2011.

[72] J. Fan, L. Batina, I. Verbauwhede, Hecc goes embedded: an area-efficient implementation of hecc, in: R.M. Avanzi, L. Keliher, F. Sica (Eds.), Selected Areas in Cryptography, Vol. 5381 of Lecture Notes in Computer Science, Springer, 2008, pp. 387–400.

[73] J. Hoffstein, J. Pipher, J.H. Silverman, Ntru: a ring-based public key cryptosystem, in: Lecture Notes in Computer Science, Springer-Verlag, 1998, pp. 267–288.

[74] M.-J.O. Saarinen, The bluejay ultra-lightweight hybrid cryptosystem, in: Proceedings of the IEEE Symposium on Security and Privacy Workshops, IEEE Computer Society, 2012, pp. 27–32.

[75] W. Che, H. Deng, W. Tan, J. Wang, A Random Number Generator for Application in RFID Tags, Springer Berlin Heidelberg, 2008, Ch. 16, pp. 279–287.

[76] J. Melia-Segui, J. Garcia-Alfaro, J. Herrera-Joancomarti, Analysis and improvement of a pseudorandom number generator for EPC Gen2 tags, in: Proceedings of the 1st International Workshop on Lightweight Cryptography for Resource-Constrained Devices – WLC'10, Lecture Notes in Computer Science, Springer, Tenerife, Canary Islands, Spain, 2010.

[77] P. Peris-Lopez, J.C.H. Castro, J.M. Estvez-Tapiador, A. Ribagorda, Lamed - a prng for epc class-1 generation-2 rfid specification, Comput. Stand. Interfaces 31 (1) (2009) 88–97.

[78] W. Che, H. Deng, W. Tan, J. Wang, A Random Number Generator for Application in RFID Tags, Springer Berlin Heidelberg, Berlin, Heidelberg, 2008, pp. 279–287, https://doi.org/10.1007/978-3-540-71641-9_16.

[79] K. Mandal, X. Fan, G. Gong, Warbler: a lightweight pseudorandom number generator for EPC C1 Gen2 passive RFID tags, Int. J. RFID Secur. Cryptogr. 2 (1) (2013) 82–91.

[80] J. Melia-Segui, J. Garcia-Alfaro, J. Herrera-Joancomarti, Analysis and Improvement of a Pseudorandom Number Generator for EPC Gen2 Tags, Springer Berlin Heidelberg, Berlin, Heidelberg, 2010, pp. 34–46, https://doi.org/10.1007/978-3-642-14992-4_4.

[81] A. Juels, R.L. Rivest, M. Szydlo, The blocker tag: selective blocking of rfid tags for consumer privacy, in: Proceedings of the 8th ACM Conference on Computer and Communications Security, ACM Press, USA, 2003, pp. 103–111.

[82] S. Ahson, M. Ilyas, RFID Handbook: Applications, Technology, Security, and Privacy, CRC Press, 2008.

[83] A. Juels, J.G. Brainard, Soft blocking: flexible blocker tags on the cheap, in: V. Atluri, P.F. Syverson, S.D.C. di Vimercati (Eds.), Proceedings of the WPES, ACM, 2004, pp. 1–7.

[84] M. Langheinrich, A survey of RFID privacy approaches, Pers. Ubiquitous Comput. 13 (6) (2009) 413–421.

[85] S.L. Garfinkel, A. Juels, R. Pappu, Rfid privacy: an overview of problems and proposed solutions, IEEE Secur. Priv. 3 (3) (2005) 34–43.

[86] M. Abu-Elkheir, M. Hayajneh, N.A. Ali, Data management for the internet of things: design primitives and solution, Sensors 13 (11) (2013) 15582–15612.

[87] Y. Zhang, L. Yang, J. Chen, RFID and Sensor Networks: Architectures, Protocols, Security, and Integrations, Wireless Networks and Mobile Communications, Taylor and Francis, 2010.

[88] Y. Sang, H. Shen, Y. Inoguchi, Y. Tan, N. Xiong, Secure data aggregation in wireless sensor networks: a survey, in: Proceedings of the Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT 2006), IEEE Computer Society, 4–7 December 2006, Taipei, Taiwan, 2006, pp. 315–320.

[89] L. Veltri, S. Cirani, S. Busanelli, G. Ferrari, A novel batch-based group key management protocol applied to the internet of things, Ad Hoc Netw. 11 (8) (2013) 2724–2737.

[90] J. van den Hoven (Chair Ethics Subgroup IoT Expert Group), Fact Sheet Ethics Subgroup IoT, version 4.0, Tech. Rep., Delft University of Technology, 2012.

[91] J.H. Cho, A. Swami, I. Chen, A survey on trust management for mobile ad hoc networks, IEEE Commun. Surv. Tutor. 13 (4) (2011) 562–583.

[92] D. Gambetta, Can We Trust Trust? Trust: Making and Breaking Cooperative Relations (electronic edition), Department of Sociology, University of Oxford, 2000, pp. 213–237.

[93] D.H. Mcknight, N.L. Chervany, The meanings of trust, Tech. Rep., 1996.

[94] S. Etalle, J. den Hartog, S. Marsh, Trust and punishment, in: F. Davide (Ed.), Autonomics, Vol. 302 of ACM International Conference Proceeding Series, ACM, 2007, p. 5.

[95] G. Suryanarayana, R.N. Taylor, A Survey of Trust Management and Resource Discovery Technologies in Peer-to-Peer Applications, Tech. Rep. uci-isr-04-6, The University of California, Irvine, California, USA, 2004.

[96] T.H. Noor, Q.Z. Sheng, S. Zeadally, J. Yu, Trust management of services in cloud environments: obstacles and solutions, ACM Comput. Surv. 46 (1) (2013) 12.

[97] S. Song, K. Hwang, Y.-K. Kwok, Trusted grid computing with security binding and trust integration, J. Grid Comput. 3 (1–2) (2005) 53–73.

[98] R. Chen, W. Yeager, Poblano A Distributed Trust Model for Peer-to-Peer Networks, Springer.

[99] B. Bhargava, A.B. Can, B. Bhargava, Sort: A Self-Organizing Trust Model for Peer-to-Peer Systems, 2006.

[100] Y. Wang, V. Varadharajan, Role-based recommendation and trust evaluation, in: Proceedings of the CEC/EEE, IEEE Computer Society, 2007, pp. 278–288.

[101] E. Damiani, S.D.C. di Vimercati, S. Paraboschi, P. Samarati, F. Violante, A reputation-based approach for choosing reliable resources in peer-to-peer networks, in: V. Atluri (Ed.), Proceedings of the ACM Conference on Computer and Communications Security, ACM, 2002, pp. 207–216.

[102] S.D. Kamvar, M.T. Schlosser, H. Garcia-Molina, The eigentrust algorithm for reputation management in p2p networks, in: Proceedings of the Twelfth International World Wide Web Conference, 2003.

[103] L. Xiong, L. Liu, Peertrust: supporting reputation-based trust for peer-to-peer electronic communities, IEEE Trans. Knowl. Data Eng. 16 (7) (2004) 843–857.

[104] R. Aringhieri, Assessing efficiency of trust management in peer-to-peer systems, in: Proceedings of the WETICE, IEEE Computer Society, 2005, pp. 368–374.

[105] M. Srivatsa, L. Liu, Securing decentralized reputation management using trustguard, J. Parallel Distrib. Comput. 66 (9) (2006) 1217–1232.

[106] R. Zhou, K. Hwang, Trust overlay networks for global reputation aggregation in p2p grid computing, in: Proceedings of the IPDPS, IEEE, 2006.

[107] X. Liu, A. Datta, A trust prediction approach capturing agents dynamic behavior, in: T. Walsh (Ed.), Proceedings of the IJCAI, IJCAI/AAAI, 2011, pp. 2147–2152.

[108] Y. Aytas, H. Ferhatosmanoglu, zgr Ulusoy, Link Recommendation in p2p Social Networks, 2012.

[109] P. Domingues, B. Sousa, L.M. Silva, Sabotage-tolerance and trust management in desktop grid computing, Future Gener. Comput. Syst. 23 (7) (2007) 904–912.

[110] F. Azzedin, M. Maheswaran, Integrating trust into grid resource management systems, in: Proceedings of the ICPP, IEEE Computer Society, 2002, pp. 47–54.

[111] F. Azzedin, M. Maheswaran, Towards trust-aware resource management in grid computing systems, in: Proceedings of the CCGRID, IEEE Computer Society, 2002, pp. 452–457.

[112] F. Azzedin, M. Maheswaran, A trust brokering system and its application to resource management in public-resource grids, in: Proceedings of the IPDPS, IEEE Computer Society, 2004.

[113] C. Lin, V. Varadharajan, Y.W. 0002, V. Pruthi, Enhancing grid security with trust management, in: Proceedings of the IEEE SCC, IEEE Computer Society, 2004, pp. 303–310.

[114] H. Kim, H. Lee, W. Kim, Y. Kim, A trust evaluation model for qos guarantee in cloud systems, Int. J. Grid Distrib. Comput. 3 (1) (2010) 1–10.

[115] K. Ramachandran, H. Lutfiyya, M. Perry, Decentralized resource availability prediction for a desktop grid, in: Proceedings of the CCGRID, IEEE, 2010, pp. 643–648.

[116] Anjali, S. Khurana, M. Sharma, Efficient grid resource selection based on performance measures, Int. J. Comput. Sci. Commun. Technol. – TECHNIA 4 (2).

[117] H. Skogsrud, B. Benatallah, F. Casati, F. Toumani, Managing impacts of security protocol changes in service-oriented applications, in: Proceedings of the ICSE, IEEE Computer Society, 2007, pp. 468–477.

[118] H. Skogsrud, H.R.M. Nezhad, B. Benatallah, F. Casati, Modeling trust negotiation for web services, IEEE Comput. 42 (2) (2009) 54–61.

[119] S. Park, L. Liu, C. Pu, M. Srivatsa, J. Zhang, Resilient trust management for web service integration, in: Proceedings of the ICWS, IEEE Computer Society, 2005, pp. 499–506.

[120] F. Skopik, D. Schall, S. Dustdar, Start trusting strangers? Bootstrapping and prediction of trust, in: G. Vossen, D.D.E. Long, J.X. Yu (Eds.), Proceedings of the WISE, Vol. 5802 of Lecture Notes in Computer Science, Springer, 2009, pp. 275–289.

[121] W. Conner, A. Iyengar, T.A. Mikalsen, I. Rouvellou, K. Nahrstedt, A trust management framework for service-oriented environments, in: J. Quemada, G. Len, Y.S. Maarek, W. Nejdl (Eds.), Proceedings of the WWW, ACM, 2009, pp. 891–900.

[122] Z. Malik, A. Bouguettaya, Rater credibility assessment in web services interactions, World Wide Web 12 (1) (2009) 3–25.

[123] Z. Malik, A. Bouguettaya, Rateweb: reputation assessment for trust establishment among web services, VLDB J. 18 (4) (2009) 885–911.

[124] Z. Malik, A. Bouguettaya, Reputation bootstrapping for trust establishment among web services, IEEE Internet Comput. 13 (1) (2009) 40–47.

[125] F. Skopik, D. Schall, S. Dustdar, Trustworthy interaction balancing in mixed service-oriented systems, in: S.Y. Shin, S. Ossowski, M. Schumacher, M.J. Palakal, C.-C. Hung (Eds.), Proceedings of the SAC, ACM, 2010, pp. 799–806.

[126] N. Santos, K.P. Gummadi, R. Rodrigues, Towards trusted cloud computing, in: Proceedings of the HOTCLOUD, 2009.

[127] J. Yao, S. Chen, C. Wang, D. Levy, J. Zic, Accountability as a service for the cloud, in: Proceedings of the IEEE SCC, IEEE Computer Society, 2010, pp. 81–88.

[128] F.J. Krautheim, D.S. Phatak, A.T. Sherman, Introducing the trusted virtual environment module: a new mechanism for rooting trust in cloud computing, in: A. Acquisti, S.W. Smith, A.-R. Sadeghi (Eds.), Proceedings of the TRUST, Vol. 6101 of Lecture Notes in Computer Science, Springer, 2010, pp. 211–227.

[129] S.M. Habib, S. Ries, M. Muhlhauser, Towards a trust management system for cloud computing, in: Proceedings of the 2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications, TRUSTCOM'11, IEEE Computer Society, Washington, DC, USA, 2011, pp. 933–939. https://doi.org/10.1109/TrustCom.2011.129.

[130] P.D. Manuel, S.T. Selvi, M.I.A.-E. Barr, Trust management system for grid and cloud resources, in: Proceedings of the International Conference on Advanced Computing, 2009. https://doi.org/10.1109/ICADVC.2009.5378187.

[131] T.H. Noor, Q.Z. Sheng, Credibility-based trust management for services in cloud environments, in: G. Kappel, Z. Maamar, H.R.M. Nezhad (Eds.), Proceedings of the ICSOC, Vol. 7084 of Lecture Notes in Computer Science, Springer, 2011, pp. 328–343.

[132] T.H. Noor, Q.Z. Sheng, Trust as a service: a framework for trust management in cloud environments, in: Proceedings of the WISE, Vol. 6997 of Lecture Notes in Computer Science, Springer, 2011, pp. 314–321.
[133] S.D.C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, G. Psaila, P. Samarati, Integrating trust management and access control in data-intensive web applications, Trans. Web 6 (2) (2012) 6.
[134] C.E. Briguez, F.M. Sagui, M. Capobianco, A.G. Maguitman, System Architecture for Trust-Based News Recommenders on the Web, in: Proceedings of the XVII Workshop de Agentes y Sistemas Inteligentes – CACIC 2011: XVII Congreso Argentino de Ciencias de la Computación, La Plata, Buenos Aires, Argentina, 2011.
[135] K. Zolfaghar, A. Aghaie, A syntactical approach for interpersonal trust prediction in social web applications: combining contextual and structural data, Knowl.-Based Syst. 26 (2012) 93–102.
[136] V.D. Gligor, J.M. Wing, Towards a theory of trust in networks of humans and computers, in: B. Christianson, B. Crispo, J.A. Malcolm, F. Stajano (Eds.), Proceedings of the Security Protocols Workshop, Vol. 7114 of Lecture Notes in Computer Science, Springer, 2011, pp. 223–242.
[137] L. Atzori, A. Iera, G. Morabito, Siot: giving a social structure to the internet of things, IEEE Commun. Lett. 15 (11) (2011) 1193–1195.
[138] M. Nitti, R. Girau, L. Atzori, A. Iera, G. Morabito, A subjective model for trustworthiness evaluation in the social internet of things, in: Proceedings of the PIMRC, IEEE, 2012, pp. 18–23.
[139] C. Pastrone, D. Rotondi, A. Skarmeta, H. Sundmaeker, O. Vermesan, S. Ziegler, P.T. Kirstein, S. Varakliotis, A. Al-Hezmi, Z. Xueli, L. Yang, T. Ye, X. Pengfei, W. Dongya, Z. Xu, M. Wenjing, Internet of things, eu-china joint white paper on internet-of-things identification, Tech. Rep., European Research Cluster on the Internet of Things, November 2014.
[140] P. Peris-Lopez, J.C.H. Castro, J.M. Estvez-Tapiador, A. Ribagorda, An ultra light authentication protocol resistant to passive attacks under the gen-2 specification, J. Inf. Sci. Eng. 25 (1) (2009) 33–57.
[141] J. Miao, L. Wang, Rapid identification authentication protocol for mobile nodes in internet of things with privacy protection, J. Netw. 7 (7) (2012) 1099–1105.
[142] R. Roman, P. Najera, J. Lopez, Securing the internet of things, Computer 44 (9) (2011) 51–58, https://doi.org/10.1109/MC.2011.291.
[143] I. Blake, G. Seroussi, N. Smart, J.W.S Cassels, Advances in Elliptic Curve Cryptography, London Mathematical Society Lecture Note Series, Springer, USA, 2005.
[144] S.B. Tom, J. Kamierski, Energy Harvesting Systems: Principles, Modeling and Applications, Springer, 2010.
[145] D.N. Duc, J. Kim, K. Kim, Scalable grouping-proof protocol for rfid tags, in: Proceedings of the Symposium on Cryptography and Information Security, Takamatsu, Japan, 2010.
[146] W.-T. Ko, S.-Y. Chiou, E.-H. Lu, H.K.-C. Chang, A privacy-preserving grouping proof protocol based on ecc with untraceability for rfid, Appl. Math. 3 (4) (2012) 336–341.
[147] G.P. Hancke, Design of a secure distance-bounding channel for rfid, J. Netw. Comput. Appl. 34 (3) (2011) 877–887.
[148] A. Fernndez-Mir, R. Trujillo-Rasua, J. Castell-Roca, J. Domingo-Ferrer, A scalable rfid authentication protocol supporting ownership transfer and controlled delegation, in: A. Juels, C. Paar (Eds.), Proceedings of the RFID, Security and Privacy – 7th International Workshop, RFIDSec 2011, Amherst, USA, June 26–28, 2011, Revised Selected Papers, Vol. 7055 of Lecture Notes in Computer Science, Springer, 2011, pp. 147–162.
[149] J.B. Rachel Greenstadt, Cognitive security for personal devices, in: Proceedings of the ACM Workshop on Artificial Intelligence and Security, ACM Conference on Computer and Communications Security, ACM, 2008, pp. 27–30.
[150] A.K. Ranjan, G. Somani, Access Control and Authentication in the Internet of Things Environment, Springer International Publishing, Cham, 2016, pp. 283–305, https://doi.org/10.1007/978-3-319-33124-9_12.
[151] K.A. McKay, L. Bassham, M.S. Turan, N. Mouha, Report on Lightweight Cryptography, draft nistir 8114, Tech. Rep., National Institute of Standards and Technology, August 2016.
[152] H.A. Maw, H. Xiao, B. Christianson, J.A. Malcolm, A survey of access control models in wireless sensor networks, J. Sens. Actuator Netw. 3 (2) (2014) 150–180, https://doi.org/10.3390/jsan3020150. ⟨http://www.mdpi.com/2224-2708/3/2/150⟩.
[153] D. Kulkarni, A. Tripathi, Context-aware role-based access control in pervasive computing systems, in: Proceedings of the 13th ACM Symposium on Access Control Models and Technologies, SACMAT'08, ACM, New York, NY, USA, 2008, pp. 113–122. https://doi.org/10.1145/1377836.1377854. ⟨http://doi.acm.org/10.1145/1377836.1377854⟩.
[154] H.A. Maw, H. Xiao, B. Christianson, J.A. Malcolm, An evaluation of break-the-glass access control model for medical data in wireless sensor networks, in: Proceedings of the 2014 IEEE 16th International Conference on e-Health Networking, Applications and Services (Healthcom), 2014, pp. 130–135 https://doi.org/10.1109/HealthCom.2014.7001829.
[155] I. Bouij-Pasquier, A.A. Ouahman, A.A.E. Kalam, M.O. de Montfort, Smartorbac security and privacy in the internet of things, in: Proceedings of the 12th IEEE/ACS International Conference of Computer Systems and Applications, AICCSA 2015, Marrakech, Morocco, November 17–20 2015, pp. 1–8. https://doi.org/10.1109/AICCSA.2015.7507098.
[156] S. Yu, K. Ren, W. Lou, Fdac: toward fine-grained distributed data access control in wireless sensor networks, IEEE Trans. Parallel Distrib. Syst. 22 (4) (2011) 673–686, https://doi.org/10.1109/TPDS.2010.130.
[157] S. Ruj, A. Nayak, I. Stojmenovic, Distributed fine-grained access control in wireless sensor networks, in: Proceedings of the 2011 IEEE International Parallel Distributed Processing Symposium, 2011, pp. 352–362. https://doi.org/10.1109/IPDPS.2011.42.
[158] J. Hur, Fine-grained data access control for distributed sensor networks, Wirel. Netw. 17 (5) (2011) 1235–1249, https://doi.org/10.1007/s11276-011-0345-8.
[159] H.A. Maw, H. Xiao, B. Christianson, An adaptive access control model for medical data in wireless sensor networks, in: Proceedings of the IEEE 15th International Conference on e-Health Networking, Applications and Services, Healthcom 2013, Lisbon, Portugal, October 9–12 2013, pp. 303–309 https://doi.org/10.1109/HealthCom.2013.6720690.
[160] R. Zhang, Y. Zhang, K. Ren, Distributed privacy-preserving access control in sensor networks, IEEE Trans. Parallel Distrib. Syst. 23 (8) (2012) 1427–1438, https://doi.org/10.1109/TPDS.2011.299.
[161] D. He, J. Bu, S. Zhu, S. Chan, C. Chen, Distributed access control with privacy support in wireless sensor networks, IEEE Trans. Wirel. Commun. 10 (10) (2011) 3472–3481, https://doi.org/10.1109/TWC.2011.072511.102283.
[162] S.T. Tim Polk, Security challenges for the internet of things, in: Proceedings of the Workshop on Interconnecting Smart Objects with the Internet, 2011.