Security, Privacy & Trust in Internet of Things: the road ahead

S. Sicari[a,*], A. Rizzardi[a], L.A. Grieco[b], A. Coen-Porisini[a]

[a] *"DISTA, Dep. of Theoretical and Applied Science", University of Insubria – v. Mazzini 5 – 21100, Varese, Italy.*
[b] *"DEI, Dep. of Electrical and Information Engineering", Politecnico di Bari – v. Orabona 4 – 70125, Bari, Italy.*

Abstract

Internet of Things (IoT) is characterized by heterogeneous technologies, which concur to the provisioning of innovative services in various application domains. In this scenario, the satisfaction of security and privacy requirements plays a fundamental role. Such requirements include data confidentiality and authentication, access control within the IoT network, privacy and trust among users and things, and the enforcement of security and privacy policies. Traditional security countermeasures cannot be directly applied to IoT technologies due to the different standards and communication stacks involved. Moreover, the high number of interconnected devices arises scalability issues; therefore a flexible infrastructure is needed able to deal with security threats in such a dynamic environment. In this survey we present the main research challenges and the existing solutions in the field of IoT security, identifying open issues, and suggesting some hints for future research.

Keywords: Internet of Things, Security, Privacy, Trust

*Corresponding author: sabrina.sicari@uninsubria.it
Email addresses: sabrina.sicari@uninsubria.it (S. Sicari), alessandra.rizzardi@uninsubria.it (A. Rizzardi), a.grieco@poliba.it (L.A. Grieco), alberto.coenporisini@uninsubria.it (A. Coen-Porisini)

1. Introduction

During the last decade, Internet of Things (IoT) approached our lives silently and gradually, thanks to the availability of wireless communication systems (e.g., RFID, WiFi, 4G, IEEE 802.15.x), which have been increasingly employed as technology driver for crucial smart monitoring and control applications [1] [2] [3].

Nowadays, the concept of IoT is many-folded, it embraces many different technologies, services, and standards and it is widely perceived as the angular stone of the ICT market in the next ten years, at least [4] [5] [6].

From a logical viewpoint, an IoT system can be depicted as a collection of smart devices that interact on a collaborative basis to fulfill a common goal. At the technological floor, IoT deployments may adopt different processing and communication architectures, technologies, and design methodologies, based on their target. For instance, the same IoT system could leverage the capabilities of a wireless sensor network (WSN) that collects the environmental information in a given area and a set of smartphones on top of which monitoring applications run. In the middle, a standardized or proprietary middleware could be employed to ease the access to virtualized resources and services. The middleware, in turn, might be implemented using cloud technologies, centralized overlays, or peer to peer systems [7].

Of course, this high level of heterogeneity, coupled to the wide scale of IoT systems, is expected to magnify security threats of the current Internet, which is being increasingly used to let interact humans, machines, and robots, in any combination. More in details, traditional security countermeasures and privacy enforcement cannot be directly applied to IoT technologies due to their limited computing power; moreover the high number of interconneted devices arises scalability issues. At the same time, to reach a full acceptance by users it is mandatory to define valid security, privacy and trust models suitable for the IoT application context [8] [9] [2] [10] [11]. With reference to security, data anonymity, confidentiality and integrity need to be guaranteed, as well as au-

thentication and authorization mechanisms in order to prevent unauthorized users (i.e., humans and devices) to access the system. Whereas, concerning privacy requirement, both data protection and users personal information confidentiality have to be ensured, since devices may manage sensitive information (e.g., user habits). Finally, trust is a fundamental issue since the IoT environment is characterized by different devices which have to process and handle the data in compliance with user needs and rights.

Note that adaptation and self-healing play a key role in IoT infrastructures, which must be able to face normal and unexpected changes of the target environment. Accordingly, privacy and security issues should be treated with a high degree of flexibility as advocated in [12] [13]. Together with the conventional security solutions, there is also the need to provide built-in security in the devices themselves (i.e., embedded) in order to pursue dynamic prevention, detection, diagnosis, isolation and countermeasures against successful breaches, as underlined in [14].

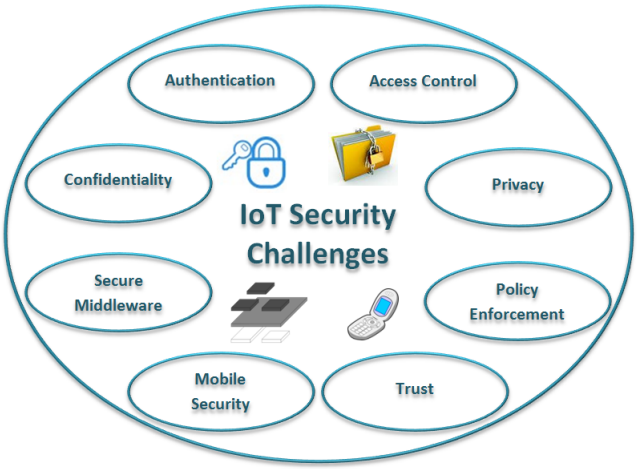

Figure 1: Main security issues in IoT

Our work analyzes the most relevant available solutions related to security (i.e., integrity, confidentiality, authentication), privacy, and trust in IoT field. We also focus on proposals regarding security middlewares and secure solutions

for mobile devices, as well as ongoing international projects on this subject. The main topics analyzed are shown in Fig. 1. In literature, other surveys deal with issues related to the IoT paradigm: [1] analyzes the IoT enabling technologies and existing middlewares, also from an application point of view, and presents security and privacy open issues together with standardization, addressing, and networking ones; [8] considers the security and privacy challenges only under a legislative point of view, with particular attention to the European Commission directives; [2] discusses the main research contexts (i.e., impact areas, projects, and standardization activities) and challenges in IoT, dealing also with data confidentiality, privacy, and trust as regards security requirements; [15] is on Internet of Underwater Things and presents only few hints to security issue; [10] investigates the advantages and disadvantages of centralized and distributed architectures in terms of security and privacy in IoT with an analysis of the principal attack models and threats; [16] provides a general overview on various IoT aspects, such as the involved technologies, the applications, the cloud platforms, the architecture, the energy consumption and security issues, the quality of service and data mining implications; [17] focuses only on the specific issue of trust management in IoT.

The contribution of this paper is compared in Table 1 with respect to the aforementioned surveys: it clearly embraces with a broaded breath all security-related facets and of course it includes more recent references on the subject.

The rest of this paper is organized as follows. Section 2 analyzes the available approaches regarding confidentiality and access control in IoT. Sections 3 and 4 deal with privacy and trust issues, respectively. Section 5 shows the security and privacy policies enforcement in IoT applications. Security middlewares are discussed in Sections 6. Section 7 addresses security in mobile IoT devices; Section 8 refers to the ongoing international projects on IoT security. Section 9 ends the paper and draws the road ahead.

Table 1: Contribution of available surveys on IoT security

	[1]	*[8]*	*[2]*	*[15]*	*[10]*	*[16]*	*[17]*	*Our work*
Security	yes	no	yes	yes	yes	yes	no	yes
Privacy	yes	yes	yes	no	yes	yes	no	yes
Trust	no	yes	yes	no	yes	no	yes	yes
Middleware	yes	no	no	no	no	no	no	yes
Mobile	no	no	no	no	no	no	no	yes
Projects	no	no	yes	no	no	no	no	yes

2. IoT security requirements: authentication, confidentiality and access control

This section analyzes in depth three key security requirements: authentication, confidentiality, and access control, with a special focus on IoT systems. IoT, in fact, enables a constant transfer and sharing of data among things and users in order to achieve particular goals. In such a sharing environment, authentication, authorization, access control and non-repudiation are important to ensure secure communication. In this context, the lack of computing resources (i.e., processing power, storage) and ad-hoc nature of such networks requires to taylor existing techniques to this new environment. In particular, the seminal contributions in such a field will be illustrated together with a critical review of open issues that deserve further investigation [10].

2.1. Authentication and Confidentiality

As regards authentication, the approach presented in [18] makes use of a custom encapsulation mechanism, namely smart business security IoT application Protocol - intelligent Service Security Application Protocol. It combines cross-platform communications with encryption, signature, and authentication, in order to improve IoT applications development capabilities by establishing a secure communication system among different things.

In [19] it is introduced the first fully implemented two-way authentication security scheme for IoT, based on existing Internet standards, specifically the Datagram Transport Layer Security (DTLS) protocol, which is placed between transport and application layer. This scheme is based on RSA and it is designed for IPv6 over Low power Wireless Personal Area Networks (6LoWPANs) [3]. The extensive evaluation, based on real IoT systems, shows that such an architecture provides message integrity, confidentiality, and authenticity with enough affordable energy, end-to-end latency, and memory overhead.

As regards confidentiality and integrity, in [20] it is analyzed how existing key management systems could be applied to the IoT context. It is possible to classify the Key Management System (KMS) protocols in four major categories: key pool framework, mathematical framework, negotiation framework, and public key framework. In [20] the authors argue that most of the KMS protocols are not suitable for IoT. In fact, key pool ones suffer insufficient connectivity; mathematical ones make use of the deployment knowledge to optimize the construction of their data structures, but such an approach cannot be used in IoT since client and server nodes are usually located in different physical locations; combinatorics-based KMS protocols suffer both connectivity and scalability/authentication; negotiation ones make use of the wireless channel and its inherent features to negotiate a common key, however they cannot be suitable for IoT because client and server nodes usually belong to different networks and they should route the information through the Internet in order to be able to talk with each other. Hence, the KMS protocols which might be suitable for some IoT scenarios are the Blom [21] and the polynomial schema [22], whose computational overhead is quite low in comparison to a Public Key Cryptography (PKC) operations (i.e., public key framework). However for such schemes, several countermeasures are required in order to manage device authentication and face man-in-the-middle attacks. For example, [23] and [24] present a framework for IoT based on Public Key Infrastructure (PKI).

A more practical approach, as [25], proposes a transmission model with signature-encryption schemes, which addresses IoT security requirements (i.e.,

anonymity, trustworthy and attack-resistance) by means of Object Naming Service (ONS) queries. Root-ONS can authenticate the identities and platform creditability of Local ONS servers (L-ONS) by a Trusted Authentication Server (TAS), and the TAS gives a temporary certificate to validated L-ONS, which can apply for inquiry services many times with the certificate in the validated time. A security ONS query service with anonymous authentication provides credentials only to authorized and trusted L-ONS, preventing the illegal ONS to enquire information from things. In the transmission process, Remote Information Server of Things (R-TIS) wraps the information of things into multiple encryption layers with the routing node's public key. The encrypted data are decrypted at each routing node, until the Local Information Server of Things (L-TIS) receives the plain text. Meanwhile, the nodes can check the integrity of received data and the creditability of routing path in the transmitting procedure. Such a transmission model results very weak in terms of attack-resistance due to the adoption of hop-by-hop encryption/decryption behavior.

It appears that an unique and well-defined solution able to guarantee confidentiality in a IoT context is still missing, as also asserted in [26]. It is worth to note that many efforts have been conducted in the WSN field [27] [28] [29] [30] [31] [32], but several questions arise:

- Are the WSN proposals adaptable to the IoT environment, considering both the heterogeneity of the involved devices and the different application contexts?
- How and at which network layer to handle authentication?
- Is it feasible to reuse the traditional security mechanisms (e.g., encryption algorithms) or it is better to start from new solutions?
- How to handle the different keys?
- Which kind of key distribution mechanism is the most suitable?
- How to ensure an end-to-end integrity verification mechanism in order to make the system more resilient to malicious attacks?

Very recent works started addressing such questions. For example, an authentication protocol for IoT is presented in [33], using lightweight encryption method based on XOR manipulation for anti-counterfeiting and privacy protection, in order to cope with constrained IoT devices.

Starting from WSN context, an user authentication and key agreement scheme for heterogeneous wireless sensor networks is also proposed in [34]. It enables a remote user to securely negotiate a session key with a sensor node, using a lean key agreement protocol. In this way, it ensures mutual authentication among users, sensor nodes, and gateway nodes (GWN), although GWN is never contacted by the user. In order to apply such a scheme to resource-constrained architectures, it only uses simple hash and XOR computations, as in [33].

The authentication and access control method presented in [35] aims at establishing the session key on the basis of Elliptic Curve Cryptography (ECC), another lightweight encryption mechanism. This scheme defines attribute-based access control policies, managed by an attribute authority, enhancing mutual authentication among the user and the sensor nodes, as well as solving the resource-constrained issue at application level in IoT.

These preliminary answers partially address afore-listed questions because they specifically target the problem of lightweight cyphering in pervasive environments. Further efforts are required to complement these lean mechanisms with stardadized protocols for authentication and a clear definition of one or more authorities aimed at guaranteeing the expected confidentiality within the IoT infrastructure.

2.2. Access control

Access control refers to the permissions in the usage of resources, assigned to different actors of a wide IoT network. Two subjects are identified in [36]: the data holders and the data collectors. Users and things, as data holders, must be able to feed data collectors only with the data regarding a specific target. At the same time, data collectors must be able to identify or authenticate users and things as legitimate data holders, from which the information are collected.

In IoT we have also to deal with processing of streaming data and not, as in traditional database systems, with discrete data. The main critical issues in this context refer to performance and temporal constraints, since access control for a data stream is more computational intensive than in traditional DBMS (DataBase Management System). In fact, queries have to be directly executed on incoming streams, which can be made of large volumes of data that might arrive at unpredictable rates. Several works deal with these aspects.

In [37] the attention is focused on the layer responsible for data acquisition, which is the direct responsible for the information collection. In such a layer, a large amount of nodes are required to sense a wide range of different data types for authorized users in accordance with privacy and security levels. Therefore [37] presents a hierarchical access control scheme for this layer. The scheme considers the limited computational and storage capacity of the nodes, in fact only a single key is given to each user and node; the other necessary keys are derived by using a deterministic key derivation algorithm,,therefore increasing the security (since the keys exchange is limited) and reducing lots of the nodes storage costs.

Starting from the consideration that in emergency situations (e.g., an accident occurs, and a doctor is needed), the location of the user can be made available, while under normal circumstances, the user's location information is confidential, [38] presents an identity based system for personal location in emergency situations. It consists of: registration, users authentication, policy, and client subsystems. The system confirms the identity of the user through the user authentication subsystem and gets the level of the emergency through the policy subsystem. Then it can make sure that user's location information can be accessed only by some authorized user and only when it is needed.

In [39] a security architecture is developed, which aims at ensuring data integrity and confidentiality, starting from a prototype query processing engine for data streams, called Nile [40]. Such a mechanism is based on FT-RC4, an extension of the RC4 algorithm, which represents a stream cipher encryption scheme, to overcome possible decryption fails due to de-synchronization prob-

lems. [40] is focalized on shared processing of window joins over data streams, in order to enhance the performance and the scalability of the DBMS.

An approach which addresses the authentication problem of outsourced data streams can be found in [41] and in [42] with CADS (Continuous Authentication on Data Streams). In this scenario it is assumed the presence of a service provider that collects data from one or more data owners, together with authentication information, and at the same time processes queries originating from many clients. The service provider returns to the clients the query results, as well as verification information, which make them able to verify the authenticity and the completeness of the received results, on the basis of the authentication information provided by the data owner.

[43] also focuses on the data outsourcing. In particular, due to the large amout of streaming data, companies may not acquire the resources for deploying a Data Stream Management Systems (DSMS). Therefore they could outsource the stream storage and delegate its processing to a specialized third-party with strong DSMS infrastructure. Naturally, this arises the trust issue: the third-party may act maliciously to increase profit. The solution is to adopt a method for stream authentication, in order to enable clients to verify the integrity and the freshness of the streaming results received from the server. Such a solution has to be very lightweight for all parties involved (e.g., WSN applications). [43] represents streams as linear algebraic queries and it is able to authenticate dynamic vector sums and dot products, as well as dynamic matrix products, by means of hash operations, modular additions/multiplications and cryptographic security functions. Such techniques may be very suitable for IoT entities, which are characterized by resources constraints in terms of energy consumption, computation and storage.

[44] proposes a semi-distributed approach. More in details, in [44] it is proposed a security framework and an access control model to secure the so called DSMSs, which extends the Borealis data stream engine [45] with security requirements. The framework exploits an owner-extended version of RBAC (Role-Based Access Control) [46], called OxRBAC. Users have to prove their

identity through a login process, consequently a session is created and a role is established for the user to perform authorized tasks. As a result, the authorization is checked by analyzing the couple user-session. It is the system itself which provides each user with the access permissions to objects, therefore users can see only the catalogue of the objects they are allowed to view. Since there can be many output streams, the system filters the tuples in order to give to the users only permitted results. Such an approach does not consider the adoption of any encryption algorithms for data streams. Note that this framework uses a single node system and not a totally distributed data stream engine. Clearly, a distributed approach would arise new issues: the output streams might be on different nodes and the currently use of ids to uniquely identify and filter the tuples have to be managed without conflicts.

Whereas, two works, [47] and [48], exploit metadata in order to guarantee the security of the tuples in the stream. In [47] it is proposed a stream-centric approach, in which the security constraints are directly embedded into data streams and not stored on the DSMS server. More in details, security metadata tuples are interleaved with the data tuples in the streams, in order to reduce the overhead. In this work, no new access control model is defined, but an enforcement mechanism suitable for streaming data, exploiting query processing. Note that, either RBAC, DAC (Discretionary Access Control) or MAC (Mandatory Access Control) can be casted in such a solution. In [47] policies on a data streams are stated by the user owning the device producing the data streams itself. This makes a user able to specify how the DSMS has to access his/her personal information (i.e., location, health conditions,...).

In [48] an extended approach is proposed, which enriches data streams with metadata called streaming tags. In this way, users are able to use a free vocabulary to add information to reported events. It supports a variety of tagging granularities, therefore users could tag streams, tuples, attributes or specific data values. A framework based on CAPE engine [49] is implemented and tested, after the definition of a proper and novel tag query language, but this solution may present some overhead and memory issues, as reported by simula-

tion results.

The work in [50] presents an enforcement to the solution provided in [51] as regards access control of streaming data, based on the Aurora data model [52]. This framework supports two types of privileges, named read and aggregate, and also two temporal constraints, named general and window. The subjects (i.e., the users) are specified according to a role-based approach, therefore permissions are associates with roles and not directly with subjects, as in RDBMS (Relational DataBase Management System). Another idea taken from RDBMS is the definition of a language independent representation for the managed object, similarly to the view concept, in order to model the high granularity levels requested by IoT applications. Queries are registered into the stream engine and continuously executed on the incoming tuples. Whenever a user submits a query, a specific component, called Query Rewriter, checks the authorization catalogues, where permissions are specified, to verify whether the query can be partially or totally executed or should be denied. In case of partially authorized queries, it is rewritten in such a way that it only contains authorized data. In order to support the query rewriting task, a set of secure operators is defined, which filters out from the results of the corresponding not-secure operators those tuples/attributes that are not accessible according to the specified access control policies.

In [53] the authors extend these two previous works in order to make their solution independent from the stream engine. Note that in general each DSMS adopts its own language; to overcome such an issue and to allow the interaction among different DSMS, in [53] a common query model is defined and then the most used operations are translated by the Deployment Module into the specific engine query language. The results of this work have been compared with other proposals. For example, with respect to [44], which has the drawback of wasting computation time when unauthorized queries are performed, it represents a better solution. [47], as [53], focuses on access control requirement for data streams, however, in [47] access control is considered from a different point of view: the privacy protection. This is due to the fact that in [47] the privacy

policies on data streams are stated by the user who owns the device which generates the data stream itself, allowing the user to specify how the DSMS has to access his/her personal information (e.g., health conditions, location); while in [53] policies are specified by the system administrator. Moreover, in [47] access control policies are not stored in the DSMS, but they are encoded via security constraints and embedded directly into data streams: this represents also a main difference with respect to [53]. In [48] a set of operators is defined, able to enforce security constraints, but it implements them only into the CAPE engine [49]; in contrast, [53] proposes a framework able to work among a wide range of different DSMSs.

While the previous works propose extended versions or acquire some features of RBAC, in [54] the authors affirm that authorization frameworks like RBAC and ABAC (Attribute Based Access Control) do not provide sufficient scalable, manageable, and effective mechanisms to support distributed systems with many interacting services and the dynamic and scaling needs of IoT context. A problem common to ACLs (Access Control Lists), RBAC and ABAC is that in these systems it is hard to enforce the principle of least privilege access. Within the European FP7 IoT@Work project [55], a Capability Based Access Control (CapBAC) was developed, which can be used to manage the access control processes to services and information with least-privilege operations. In CapBAC it is the user that has to present his/her authorization capability (and demonstrate he/she is the owner of it) to the service provider, while in a traditional ACL system it is the service provider that has to check if the user is, directly or indirectly (e.g., via a role owned by the user), authorized to perform the requested operation on the requested resource. The authorizations are given by the owner of a certain resource/service to the desired users, which as a consequence can prove their capability to access to the resource or benefit of the service. It is stressed the relevance of security mechanisms usability and access rights delegation and the need to take into account that they have to be understandable and usable by non ICT-skilled users. It is also important to grant the principle of least privilege by default and to make possible to revoke capabilities

and to set a validity condition under which the authorization is available.

From the discussion about these works the major challenges related to access control in an IoT scenario which emerge are:

- How to guarantee the access permission in an environment where not only users, but also things could be authorized to interact with the system?
- It is more effective to exploit a centralized or distributed approach or a semi-distributed one in order to manage the scalable IoT architecture?
- How to handle the huge amount of transmitted data (i.e., in the form of stream data) in a common recognized representation?
- How to support the identification of entities?

In fact, as regards identification, one of the principal changes today is the increase in mobility of portable and powerful wireless devices. Identity requirement is not yet adequately met in networks, especially given the emergence of ubiquitous computing devices. Addressing identity issue requires to reformulate the architecture for naming, addressing and discovery and the development of specific identity management framework for IoT [56]. Only few solutions have been proposed related to such an issue. Furthermore:

- To manage access control, how could IoT system deal with the registration of users and things and the consequent issuance of credentials or certificates by authorities?
- Could the users/things present these credentials/certificates to the IoT system in order to be allowed to interact with the other authorized devices?
- Could a following step be the definition of specific roles and functions within the IoT context, in order to manage the authorization processes?

As regards the raised questions, few new solutions have been recently proposed, suggesting a subscriber method and a group membership scheme to deal with the access control of heterogeneous devices. [57] addresses authentication

and access control in the IoT framework. The proposed authorization scheme for constrained devices combines Physical Unclonable Functions (PUF) with Embedded Subscriber Identity Module (eSIM). The former provides cheap, secure, tamper-proof secret keys to authentify constrained M2M devices. The latter provides mobile connectivity guaranteeing scalability, interoperability and compliance with security protocols.

Multicast communication are secured in [58] by adopting a common secret key, denoted as group key, shared by multiple communication endpoints. Such keys are managed and distributed with a centralized batch-based approach. Note that such a mechanism reduces the computational overhead and network traffic due to group membership changes, caused by users joins and leaves, as happens in a typical IoT context. Such a protocol can be applied to two several relevant scenarios: (i) secure data aggregation in IoT and (ii) Vehicle-to-Vehicle (V2V) communications in Vehicular Ad hoc Networks (VANETs).

Finally, in [59] a general UML conceptual model suitable for all the IoT applications and architectures is defined. It specifies both involved entities and their relationships within the IoT infrastructure, pointing out their roles and functions. Also an application case-study is described, in which users and nodes interact with an IoT platform in order to obtain and/or provide customized services. Such a model takes into account the registration phase carried out by users towards the IoT platform, the consent acquisition for handling their personal data, and the exchange of the credentials for future interactions. This represents a further step towards the management of registered users and things and the relative credentials, but considerable efforts are still required to establish a standardized and globally accepted solution.

3. Privacy in IoT

IoT finds application in many different fields, for example: patients remote monitoring, energy consumption control, traffic control, smart parking system, inventory management, production chain, customization of the shopping at the

supermarket, civil protection. For all of them, users require the protection of their personal information related to their movements, habits and interactions with other people. In a single term, their privacy should be guaranteed. In literature, there are some attempts to address such an issue.

In [60] a data tagging for managing privacy in IoT is proposed. Using techniques taken from the Information Flow Control, data representing network events can be tagged with several privacy properties; such tags allow the system to reason about the flows of data and preserve the privacy of individuals. Although exploiting tagging within resource-constrained sensor nodes may not be a viable solution because tags may be too large with respect to the data size and sensitivity, therefore they generate an excessive overhead. Clearly, in this case it is not suitable for IoT.

In [61] a user-controlled privacy-preserved access control protocol is proposed, based on context-aware k-anonymity privacy policies. Note that privacy protection mechanisms are investigated: users can control which of their personal data is being collected and accessed, who is collecting and accessing such data, and when this happens.

In [62] it is presented Continuously Anonymizing STreaming data via adaptive cLustEring (CASTLE). It is a cluster-based scheme which ensures anonymity, freshness, and delay constraints on data streams, thus enhancing those privacy preserving techniques (e.g., k-anonymity) that are designed for static data sets and not for continuous, unbounded, and transient streams. More in details, [62] models k-anonymity on data streams and defines k-anonymized clusters exploiting the quasi-identifier attributes of tuples in order to preserve the sensitive data privacy.

In [63], the traditional privacy mechanisms are divided into two categories: Discretionary Access and Limited Access. The former addresses the minimum privacy risks, in order to prevent the disclosure or the cloning of sensitive data; whereas the latter aims at limiting the security access to avoid malicious unauthorized attacks.

[64] analyzes the privacy risk that occurs when a static domain name is

assigned to a specified IoT node. In this work the authors propose a privacy protection enhanced DNS (Domain Name System) for smart devices, which can authenticate the original users identity and reject illegal access to the smart device. The scheme is compatible with widely used DNS and DNSSEC (Domain Name System Security Extensions) protocols.

In [36] it is presented a fully decentralized anonymous authentication protocol for privacy-preserving target-driven IoT applications. Such a proposal is based on a multi-show credential system where different showings of the same credential cannot be linked together, therefore avoiding the generating keys to be discovered. The system defines two possible roles for participant nodes: users, which represent the nodes originating the data and data collectors, which are responsible for gathering the data from authorized users. Users can anonymously and unlinkably authenticate themselves in front of data collectors proving the owning of a valid Anonymous Access Credential (AAC) encoding a particular set of attributes, established by the system itself. The protocol is divided in three phases: set-up, user registration, during which users obtain Anonymous Access Credentials, and Credential Proving, during which users prove the possession of a valid AAC to a data collector. Such a protocol guarantees: user anonymity, AAC unlinkability (no Data Collector or set of colluding Data Collectors can link two transactions to the same User), resistance to user impersonation, faulty and selfish nodes, nodes hindering the efficiency, and adversary controlling the Data Collectors. Moreover, such a system relies on a fully distributed approach, thus avoiding single point of failure issues.

[65] analyzes in depth the performances of the two major types of Attribute-Based Encryption (ABE): Key-Policy Attribute-Based Encryption (KP-ABE) and Ciphertext-Policy Attribute-Based Encryption (CP-ABE). Simulations are carried on different classes of mobile devices, including a laptop and a smartphone, in order to establish under what conditions ABE is better suited for IoT. ABE provides a public key encryption scheme which enables a fine-grained access control, a scalable key management, and a flexible data distribution.

Another approach which uses an attribute-based signature scheme to guar-

antee privacy in IoT is presented in [66]. Here a novel Attribute-Based Signature (ABS) scheme, named ePASS, uses an attribute tree and expresses any policy consisting of AND/OR, which are unforgeable for the computational Diffie-Hellman assumption. In fact, users cannot forge signatures with attributes they do not own, and the signature provides assurance that only a user with appropriate attributes satisfying the policy can endorse the message. Moreover, the legitimate signers remain anonymous and are indistinguishable among all users whose attributes satisfy the policy, which provides attribute privacy for the signer.

Focusing on the privacy protection in IoT, [67] puts forward a key-changed mutual authentication protocol for WSN and RFID systems. Such a protocol integrates a random number generator in the tag and the reader, and adopts the one-way hash function, the key refresh in real time, and the key backup as mechanisms to reduce the risks of replay, replication, denial of service, spoofing and tag tracking.

[68], starting from the privacy preserving data mining (PPDM) techniques, aims at minimizing the sensitive data disclosure probability and the sensitive content analysis. In such a work, the user privacy awareness issue is addressed, proposing a privacy management scheme which enables the user to estimate the risk of sharing sensitive data. It also aims at developing a robust sensitivity detection system, able to quantify the privacy content of the information.

The assessment of privacy requirements of data, provided by different sources, is dealt in [69], which defines a layered architecture for IoT in order to estimate both the data quality and the security and privacy level. Moreover, such an architecture defines an annotated data for providing services, that integrates data from different sources, according to customer needs.

To summarize, privacy requirement in IoT is currently only partially covered and there is a wide space of research issues to be investigated, referring to the need to define privacy policies starting from a well-defined model [59] and the correspondent development, dealing with the scalability and the dynamic environment which characterizes IoT scenarios. In fact, capturing privacy require-

ment in the very early stages of development is essential for creating sufficient public confidence and facilitate the adoption of novel IoT systems.

4. Trust in IoT

The trust concept is used in various contexts and with different meanings. Trust is a complex notion about which no definitive consensus exists in the scientific literature, although its importance is widely recognized. A main problem with many approaches towards trust definition is that they do not lend themselves to the establishment of metrics and evaluation methodologies. Moreover, the satisfaction of trust requirements are strictly related to the identity management and access control issues.

Works [70] and [71] focus on trust level assessment of IoT entities. The authors assume that most smart objects are human-carried or human-related devices, so they are often exposed to public areas and communicate through wireless, hence vulnerable to malicious attacks. Smart objects have heterogeneous features and need to cooperatively work together. The social relationships considered are: friendship, ownership and community, since users are friends among themeselves (i.e., friendship), users own the devices (i.e., ownership) and the devices belong to some communities (i.e., community). Malicious nodes aim at breaking the basic functionality of IoT by means of trust related attacks: self-promoting, bad-mouthing and good-mouthing. The trust management protocol for IoT proposed in [70] is distributed, encounter-based, and activity-based: two nodes that come in touch to each other or involved in a mutual interaction can directly rate each other and exchange trust evaluation about the other nodes, so they perform an indirect rate which seems like a recommendation. The reference parameters to trust evaluation are: honesty, cooperativeness, and community-interest. Therefore such a dynamic trust management protocol is capable of adaptively adjusting the best trust parameter setting in response to dynamically changing environments in order to maximize application performance.

A similar approach to provide a trustworthiness evaluation is carried out in

[72] in the so called Social Internet of Things (SIoT). This paradigm derives from the integration of social networking concepts into IoT, due to the fact that the objects belonging to the IoT infrastructure are capable of establishing social relationships in an autonomous way with respect to their owners. The challenge addressed in [72] is to build a reputation-based trust mechanism for the SIoT which can effectively deal with certain types of malicious behaviors aimed at misleading other nodes, in order to drive the use of services and information delivery only towards trusted nodes. A subjective model for the management of trustworthiness is defined, which builds upon the solutions proposed for P2P networks, such as those proposed in [73] [74] [75] [76] [77]. Each node computes the trustworthiness of its friends on the basis of its own experience and on the opinion of the common friends. As a consequence, a node chooses the provider of the service it needs on the basis of this highest computed trustworthiness level.

Yet in relation to the social network context, in [78] the authors propose a secure distributed ad-hoc network; it is based on direct peer-to-peer interactions and communities creation in order to grant a quick, easy and secure access to users to surf the Web; thus close to the social network concept. Each node (i.e., device) and community have an identity in the network and modify the trust of other nodes on the basis of their behavior, thus establishing a trust chain among users. The parameters analyzed are: physical proximity, fulfillment, consistency of answer, hierarchy on the trusted chain, similar properties (e.g., age, gender, type of sensor), common goals and warrants, history of interaction, availability, interactions. Chains of confidence will allow the establishment of groups or communities and unique identities (for the communities) for the access to services as well as for the spreading of group information. Therefore security is established when the users access the network through the use of the trust chain generated by nodes, which he/she crosses.

In [79] it is considered that the traditional access control models are not suitable for the decentralized and dynamic IoT scenarios, where identities are not known in advance. Trust relationship between two devices helps in influencing

the future behaviors of their interactions. When devices trust each other, they prefer to share services and resources. This is the same idea emerged in [72] and [70]. Such a paper presents a Fuzzy approach to the Trust Based Access Control (FTBAC). The trusts scores are calculated by the FTBAC framework from factors like experience, knowledge and recommendation. Such trust scores are then mapped to permissions, and access request are accompanied by a set of credentials which together constitute a proof for allowing the access or not.

FTBAC framework is composed by three layers:

- Device Layer: includes all IoT devices and communication among these devices
- Request Layer: is mainly responsible for collecting experience, knowledge and recommendation information and calculating fuzzy trust value
- Access Control Layer: is involved in decision making process and maps the calculated fuzzy trust value to the access permissions, with the principle of least privilege.

The simulation results show that this framework guarantees flexibility and scalability and it is energy efficient. In fact, a solution based on cryptographic protection can achieve access control by increasing the trust level, but it creates extra overhead in terms of time and energy consumption; instead, according to authors, the fuzzy approach is easier to integrate in utility-based decision making.

In [80] it is presented another fuzzy approach to trust evaluation, based on three layers: sensor layer, core layer, and application layer. The sensor layer includes physical devices (e.g., RFID, WSN and base stations); the core layer mainly includes access network and Internet; the application layer includes various distributed networks (e.g., P2P, Grid, Cloud Computing), application systems and interfaces. From point of view of users, IoT system is regarded as a Service Provider (SP) and the trust management aims at providing an auxiliary service that assists the IoT to provide more qualified service to any Service

Requester (SR). The relationship is bidirectional as the trust mechanism has effects both on the SR (for privacy protection) and SP. Such trust management model mainly includes three steps: trust extraction, trust transmission, and trust decision-making. Requested information service and trust based service coexist in this model. Trust management should act as self-organizing component in order to deal with the information flow and preventing the privacy information from leaking to un-trusted SR. The authors in [80] make use of fuzzy set theory and formal semantics-based language to perform the layered trust mechanism, evaluated by using specific layer attributes (i.e., efficiency, risk, history). The user has access to the IoT only if security credential satisfies security policies, which are defined by means of a decision-making function according to user trust value. Note that, such a work discusses no concrete trust models, but establishes only a general framework, in which the well-defined trust models can be integrated.

[81] and [82] propose a trust model to protect the user security by combining location-aware and identity-aware information and authentication history; as a consequence, the users can obtain the trustworthiness for the requested services. Three trust regions are considered, each one having high, medium, and low ranks, respectively. For each rank, the authentication approach is different. In high rank case, no extra key is needed (already sign on the VID). For medium rank, users have to offer their PIN for login. Low rank means that users need to provide biometric information, such as face image, fingerprint or iris scan, which may be not convenient for its complexity and hardware constraints. The goal is to make a classification of the provided services in order to evaluate the sensitivity of the trasmitted information (i.e., on the basis of the type of application or the host in which the application is executed); for achieving such an issue, a fuzzy approach is exploited.

Other proposals are not based either on the social networking concept nor on fuzzy methods. For example, in [83] the authors propose a hierarchical trust model for IoT, able to effectively detect malicious organizations from the behavior of their neighboring nodes. A Verifiable Caching Interaction Digest (VCID)

scheme is introduced for the purposes of monitoring object-reader interaction and a long-term reputation mechanism is used to manage the trust of organizations.

[84] proposes a trust management system for IoT able to assess the trust level of a node from its past behaviour, in distinct cooperative services. The main goal of this solution is to manage cooperation in a heterogeneous IoT architecture taking into account the different nodes capabilities by exploiting a decentralized approach. Such a model considers both first-hand information (i.e., direct observations and own experiences) and second-hand information (i.e., indirect experiences and observations reported by neighboring nodes) to update trust values. Different phases are involved, in which the trust management system: (i) gathers information about the trustworthiness of the available nodes; (ii) sets up a collaborative service with the requesting nodes; (iii) learns from its past operation by performing self-updates aimed at improving its future operations; (iv) assigns a quality recommendation score to each node after each interaction during the learning phase.

In [85] the authors make an attempt to design an attack-resistant trust management model for distributed routing strategy in IoT. Such a model can evaluate and propagate reputation in distributed routing systems and it is then proposed to establish reliable trust relations between self-organized nodes and defeat possible attacks in distributed routing systems.

[86] starts from WSNs and defines a trust management for IoT, consisting in an identity-based key agreement; this agreement occurs by means of a distributed self-organizing key negotiation process. Such a protocol aims at preventing attacks from outside the network and recognizing malicious nodes. Thus it can reduce communications with malicious nodes to improve security and extend network lifetime.

[87] presents an identity-based network protocol aimed at identifying network nodes which move themselves from a host-to-host during the handover processes. Therefore it needs to decouple identifiers and locators in order to separate the node identification from host addressing. The mutual authentica-

tion of network nodes is achieved by the validation of the identity attributes and then by attaching a signature to each attribute, emitted by a trusted signing entity. Access to non-public identity information is regulated by policies defined by the owner of the information. Thus, it is disclosed only to the authorized subjects by using the same attribute-based authorization method. Nodes and a Domain Trusted Entity are connected to each other to build a globally trusted infrastructure by the pre-sharing of cryptographic certificates and ensuring the confidentiality and authentication of their exchanges by means of encryption and signature mechanisms.

As pointed out in [88] , current trust and reputation management approaches usually offer rigid and inflexible mechanisms to compute reputation scores, which hinder their dynamic adaptation to the current environment where they are deployed. At most, they provide certain parameters which are configurable or tunable. This seems not enough for the heterogeneous and dynamic IoT context. Therefore, [88] has designed and prototyped a flexible mechanism to select the most suitable trust and reputation model in heterogeneous environments. Such a mechanism can be applied on-the-fly, amongst a pool of predefined ones, considering the current system conditions (e.g., number of users, allocated resources).

A layered IoT architecture for trust management control mechanism is proposed in [89]. The IoT infrastructure is decomposed into three layers, which are: sensor layer, core layer and application layer. Each layer is controlled by a specific trust management under the following purposes: self-organization, routing and multi-service, respectively. The final decision-making is executed by the service requester (i.e., the user) according to the collected trust information as well as requester policy. A formal semantics-based and the fuzzy set theory are used to realize the trust mechanism.

Another trust system is proposed in [90], based on node behavior detection. The metrics periodically evaluated are recommended trust and history statistical trust. They are calculated by evidence combination and Bayes algorithm, respectively.

Table 2: Summary of related works on trust assessment

Exploited technique	**Works**
Social networking	[70] [71] [72] [78]
Fuzzy technique	[79] [80] [81] [82] [89]
Cooperative approach	[83] [84] [85] [90]
Identity-based method	[86] [87]

Such an overview shows that the available solutions exploit different techniques in order to handle the trust issue in IoT scenario. Such proposals include hierarchical model, reputation mechanisms, approaches derived from social networking, fuzzy techniques, mechanisms based on nodes past behavior or on routing strategies (a scheme of analyzed works is showed in Table 2). Literature seems mature enough concerning trust management, but the definition of a fully distributed and dynamic approach suitable for the scalable and flexible IoT context is still missing, as confirmed in the recent survey on trust management in IoT provided in [17]. Further missing items are the definition of globally accepted certification authorities and of a common-accepted trust negotiation language. To sum up, the following issues are still open in IoT-trust management:

- The introduction of a well-defined trust negotiation language supporting the semantic interoperabilty of IoT context
- The definition of a proper object identity management system
- The development of a trust negotiation mechanism in order to handle data stream access control.

5. Enforcement in IoT

Policy enforcement refers to the mechanisms used to force the application of a set of defined actions in a system. More in details, policies are operating

rules which need to be enforced for the purpose of maintaining order, security, and consistency on data. With reference to IoT scenarios, in literature are still present neither viable solutions nor detailed analysis on this subject. Only few works describe how to manage policies enforcement.

[91] provides an overview of network security, security policies, policy enforcement and firewall policy management systems. As regards policy enforcement, it is proposed to use security services such as authentication, encryption, antivirus software and firewalls, in order to protect the data confidentiality, integrity, and availability.

In [92] the languages regarding the definition of obligations and policies are classified into two categories. On the one hand, there are policy enforcement languages, which generally simplify the specification and interpretation of policies; however, they lack the formal semantics needed to allow the verification of the policies themselves by means of formal proofs. On the other hand, there are policy analysis languages, which allow the formal policies analysis and the expression of a large variety of obligations. In this work, it is introduced a policy language which aims at combining the advantages of both policy enforcement and analysis languages. Formalizing policy enforcement has several advantages: it reduces the gap between the specified policies and their deployment, thus it ensures that the policies are correctly applied in the system. To formalize policy enforcement, the target system should be modeled and then the effects of the application of the policies should be described. More in details, policies are enforced using reference monitors, and a set of active rules specifies that a set of actions should be executed after the detection of some events, if some conditions are met. However, this language does not provide the operational semantics needed to dynamically enforce and manage obligations in a policy managed system.

[93] pays its attention to the various types of policy languages, such as WS-Policy (Web Services-Policy) and XACML (eXtensible Access Control Markup Language), exploited in different systems. In fact, low-level enforcement mechanisms can vary from system to system. Thus, it is difficult to enforce a policy

across domain boundaries or over multiple domains. Before applying policies across domain boundaries, it is desirable to know which policies can be supported by other domains, which are partially supported, and which are not supported. In [93] it is proposed and implemented a simulation environment using semantic model mapping and translation for policy enforcement across domain boundaries by means of a semantically-rich language: Web Ontology Language (OWL), which can be used to model both policy languages and enforcement mechanisms. For example, in a healthcare environment, the cooperation and communication between pharmacy, hospital and medical school are essential. They have their own policy enforcement mechanisms to protect their own proprietary data and patients records. The problem is that there are more and more collaborations and communications among these domains, therefore a cross-domain policy enforcement becomes an essential component. However, in most cases, these domains use different policy languages to define their policies and these specific policies are executed on their own platforms. When a new cooperation or communication is required between two stranger domains, we do not know how many policy rules from the stranger domain can be enforced by current enforcement mechanisms. So in most cases, the technical departments from these two domains have to work together to evaluate whether or not it is possible to make their systems interoperating. The same problem also exists in social networking environment (e.g., Facebook, MySpace, Linkedin). Most existing social networking sites have privacy configurations based on their own enforcement mechanisms. When two social networking sites or two healthcare domains need to communicate or collaborate with each other, they have to rebuild or reconfigure their systems to make sure these activities are consistent with their own and their partners policies.

Expressing security policies to govern distributed systems is a complex and error-prone task. Because of their complexity and of the different degrees of trust among locations in which code is deployed and executed, it is challenging to make these systems secure. Moreover, policies are hard to understand, often expressed with unfriendly syntax, making it difficult for security administrators

and for business analysts to create intelligible specifications. In [94] it is introduced a Hierarchical Policy Language for Distributed Systems (HiPoLDS), which has been designed to enable the specification of security policies in distributed systems in a concise, readable and extensible way. HiPoLDS design focuses on decentralized execution environments under the control of multiple stakeholders. It represents policy enforcement through the use of distributed reference monitors, which control the flow of information among services (i.e., SOAs) and have the duty to put into action the directives output by the decision engines. For example, an enforcement engine should be able to add or remove security metadata such as signatures or message authentication codes, encrypt confidential information, or decrypt it when it is the case.

In [95] the focus is on the enforcement of privacy issues in e-commerce applications (e.g., eBay). There exist two main paradigms to protect the customer privacy: one relies on the customer trustworthiness; the other one insists on the customer anonymity. The proposed paradigm hides the customer real identity and only data which cover the actual resources he/she is looking for are allowed to circulate. Such data will be orchestrated through the network to raise potential matches, and each node will use certified email to send the customer a matching offer in a standardized format.

[96] introduces a formal and modular framework allowing to enforce a security policy on a given concurrent system. In fact, one of the important goals of the software development process is to prove that the system always meets its requirements. To deal with this problem, two different approaches are proposed. The former is a conservative enforcement: the program should be terminated as soon as it violates the security policy even if the current run could be partially completed. The latter is a liberal enforcement: the execution of the process is not aborted if it could be partially satisfied. With this approach, more properties are enforced than with the conservative one, but the program may terminate without fully satisfying the security policy. Therefore the conservative enforcement will generate fault negative, while the liberal enforcement will generate fault positive and no one of them reach the desired result. In [96] the liberal

enforcement is developed, which can be further extended to handle the conservative approach. More in details, an extended version of the Algebra for Communicating Process (ACP) [97], designed for specifying concurrent systems behavior, and the Basic Process Algebra (BPA) language for the specification of security policies are exploited. To achieve the goal, ACP is enhanced with an enforcement operator, whose actions run in parallel with the system, in order to monitor the requests and the satisfaction of the related policies.

In [98] it is proposed a novel access control framework, named Policy Machine (PM). It is composed by the following basic entities: authorized users, objects, system operations, and processes. Users may be either human beings or system users; objects specify system entities which are controlled under one or more policies (e.g., records, files, e-mails); operations identify the actions that can be performed on the contents of objects (e.g., read, write, delete); finally users submit access requests through processes. Policies are grouped in classes according to their attributes and, therefore, an object may be protected under more than one policy class, and, similarly, a user may belong to more than one policy class. In such a way PM is a general purpose protection machine, since it is able to configure many types of access control policies, and it is independent from the different operating systems and applications; users need to login only to the PM in order to interact with the secure framework. [98] demonstrates the PM ability to express and enforce the policy objectives of RBAC [46], Chinese Wall [99], MAC and DAC models [100]. Moreover, PM is able to face many Trojan horse attacks, to which DAC and RBAC are vulnerable.

Hence, [101] introduces a semantic web framework and a meta-control model to orchestrate policy reasoning with the identification and access of the sources of information. In fact, in open domains, enforcing context-sensitive policies require the ability to opportunistically interleave policy reasoning with the dynamic identification, selection, and access of relevant sources of contextual information. Each entity (i.e., user, sensor, application or organization) relies on one or more Policy Enforcing Agents responsible for enforcing relevant policies in response to incoming requests.

The authors of [102] consider that the application logic, embodied in the system components, should be separated from the related policies. Therefore, they study an infrastructure which can enable policy, representing high-level (i.e., user) or systems concerns, to drive system functionality in a distributed environment. To this end, a middleware is introduced, able to support a secure and dynamic reconfiguration, and to provide a policy enforcement mechanism across system components.

The enforcement solution presented in [103] is based on a Model-based Security Toolkit named SecKit, which is integrated with the MQ Telemetry Transport (MQTT) protocol layer, a widely adopted technology to enable the communication among IoT devices. In such a work, authorizations and obligations are identified and a specific module (i.e., Policy Enforcement Point) acts as a connector to intercept the messages exchanged in the broker with a publish-subscribe mechanism; the available enforcement actions which can be executed to cope with the received requests are: allow, deny, modify, and delay.

Note that, at the state of the art, except for the work in [103], there are no specific solutions for IoT able to guarantee the enforcement of security and privacy policies, although they are essential to ensure a safe deployment of IoT paradigm. Note that it is important to identify the enforcement mechanisms suitable for the specific IoT context, finding an equilibrium between the guarantee of security and privacy issues and the computing efforts requested by the exploited mechanisms themselves. Some efforts have already been done to define the proper languages for the specification of privacy policies, but a standard which addresses specifically IoT paradigm is still missing.

6. Secure Middlewares in IoT

Due to the very large number of heterogeneous technologies normally in place within the IoT paradigm, several types of middleware layer are employed to enforce the integration and the security of devices and data within the same information network. Within such middlewares, data must be exchanged respecting

strict protection constraints. Moreover, in middleware design and development, the different communication mediums for wide scale IoT deployments need to be considered; in fact, while many smart devices can natively support IPv6 communications [3] [104], existing deployments might not support the IP protocol within the local area scope, thus requiring ad hoc gateways and middlewares [5].

Both the networking and security issues have driven the design and the development of the VIRTUS Middleware [105], an IoT middleware relying on the open eXtensible Messaging and Presence Protocol (XMPP) to provide secure event-driven communications within an IoT scenario. Leveraging the standard security features provided by XMPP, the middleware offers a reliable and secure communication channel for distributed applications, protected with both authentication (through TLS protocol) and encryption (SASL protocol) mechanisms.

[106] proposes an AmI framework, called Otsopack. This solution provides two core features: (i) it is designed to be simple, modular and extensible and (ii) it runs in different computational platforms, including Java SE and Android. The underlying interface is based on HTTP and uses a REpresentational State Transfer (REST) interface. Different implementations can provide only certain features (e.g., data access) and still interact with each others. In this way it is possible to embed it in other devices. This gateway platform only supports Python and requires a partial ad hoc implementation. It uses a TSC (Triple Space Computing), that is a coordination paradigm which promotes the indirect communication style and uses semantic data. The way it works is simple: each application writes semantically annotated information in a shared space, and other applications or nodes can query for it. As regards security, given the data-centric nature of the framework, there are mainly two core requirements: (i) a data provider may only grant access to certain data to a certain set of users and (ii) a data consumer may trust only a set of providers for certain set of acquired data. A derived issue is how to authenticate each other in such a dynamic scenario. In order to support the first requirement, an OpenID-based

solution has been built. An Identity Provider securely identifies data consumers to the data providers. Data providers can establish which graphs can be accessed by which users. Therefore, the provider will return a restricted graph only if the valid user is requesting it. In other words, the same application can get different amounts of information depending on whether it provides credentials or not.

In [107], a framework is proposed for enhancing security, privacy and trust in embedded system infrastructures. The authors suggest the use of lightweight symmetric encryption (for data) and asymmetric encryption protocols (for key exchange) in Trivial File Transfer Protocol (TFTP). The target implementation of TFTP is the embedded devices such as Wi-Fi Access Points (AP) and remote Base Stations (BS), which should be attacked by malicious users or malwares with the installation of malicious code (e.g., backdoors). [107] emphasizes on finding a solution for strengthening the communication protocol among AP and BS. To verify this proposal, the authors decided to use UBOOT (Universal Boot loader). In [107] two schemes are implied: AES, used to protect personal and sensitive data, and DHKE (Diffie-Hellman Key Exchange), for exchanging cryptographics keys between two entities that do not know each other.

In [108] is presented a Naming, Addressing and Profile Server (NAPS) as a middleware to bridge different platforms in IoT environments. Given massive amount of heterogeneous devices deployed across different platforms, NAPS serves as key module at the back-end data center to aid the upstream, the content-based data filtering and matching and the downstream from applications. [108] proposes a novel naming convention for devices and device groups across different platforms. While previous research efforts only focus on a specific standard or protocol, the authors aim at designing a middleware component serving dynamic application needs. Therefore, an IoT Application Infrastructure (IoT-AI) is designed, which key technical components are: application gateway, service registration portal and Real-time Operational DataBase (RODB) and protocols like Universal Plug and Play (UPnP). The provided interfaces are based on the RESTful design style where standard HTTP request/response

is used to data transport. When device profile information is registered either manually or automatically from each IoT platform, an identifier is automatically generated. The system deals with Authentication, Authorization and Accounting (AAA). Although it is not the focus of this work, the design can largely leverage the Network SEcurity Capability (NSEC) SC in ETSI M2M service architecture. Note that the device domain is organized in a tree structure. It uses a key hierarchy, composed of root key, service key and application keys. Root key is used to derive service keys through authentication, and key agreement between the device or gateway and the M2M SCs at the M2M Core. The application key, derived from service key, is unique for M2M applications.

OneM2M [109] proposes a global service layer platform for M2M communications. It aims at unifying the Global M2M Community, by enabling the interoperability of different M2M systems, across multiple networks and topologies on top of IP. The presented middleware is able to support secure end-to-end data transmissions among the M2M devices and the customer applications. Such a goal is obtained by means of authentication, encryption, connectivity setup, buffering, synchronization, aggregation and device management.

Several recent works tried to address the presented issues. For example [110] deals with the problem of task allocation in IoT. More in details, the cooperation among nodes have to perform an interoperability towards a collaborative deployment of applications, able to take into account the available resources, such as energy, memory, processing, and object capability to perform a given task. In order to address such an issue, a resource allocation middleware for the deployment of distributed applications in IoT is proposed. Starting from this component, a consensus protocol for the cooperation among network objects in performing the target application is added, which aims to distribute the burden of the application execution, so that resources are adequately shared. Such a work exploits a distributed mechanism and demonstrates better performance than its centralized counterpart.

Also middlewares currently lacks an unified vision, able to responding to all the IoT requirements, both in terms of security and privacy and network

performance. Moreover, interoperability is becoming a fundamental challenge, in order to allow an independent development of distributed components, able to interact and cooperate with each other and also to exchange data on the basis of standards. Taking in mind that IoT involves not only data provided by devices/machines, but also by users, besides the interactions are machine-to-machine and also among users and machines and among users and users. Therefore, the design and development of a middleware have an impact on the system architecture (i.e., scalability, coupling among components). To design an effective solution, it occurs to deal with several important questions:

- How heterogeneous devices and users can dynamically interact and agree on the same communication protocols, ensuring also security and privacy?
- How to make the solution suitable for different platforms and therefore not dependent either on the exploited interfaces or protocols?

The work presented in [111] defines a method to deduce the process for the systematical construction of a general-purpose middleware for IoT. The middleware is generated starting from high level algebraic structures, then they are mapped into building components depending on the underlying computing infrastructure, therefore it is adaptable to heterogeneous systems.

Finally, [112] proposes a security architecture for an IoT transparent middleware. Its protection measures are based on existing technologies for security, such as AES, TLS and oAuth. In this way, the privacy, authenticity, integrity and confidentiality of exchanged data are integrated to provide security for smart objects, services and users.

7. Mobile security in IoT

Mobile nodes in IoT often move from one cluster to another, in which cryptography based protocols are required to provide rapid identification, authentication, and privacy protection. An ad-hoc protocol is presented in [113] exploited when a mobile node joins a new cluster. Such a protocol contains a valid

request message and an answer authentication message, which rapidly implements identification, authentication, and privacy protection. It could be robust towards replay attack, eavesdropping, and tracking or location privacy attacks. Compared with other similar protocols such as basic hash protocol, it has less communication overhead, more security and more privacy protection properties.

[114] analyzes the security challenges for the HIMALIS (Heterogeneity Inclusion and Mobility Adaptation through Locator ID Separation) architecture regarding features from IoT and the ID/Locator management messages, vulnerable to attacks. This work proposes a secure and scalable mobility management scheme which considers the IoT constraints, solving the possible security and privacy vulnerabilities of the HIMALIS architecture. The proposed scheme supports scalable interdomain authentication, secure location update, and binding transfer for the mobility process.

Furthermore, Radio Frequency Identification (RFID) systems, based on EPC (Electronic Product Code) Network Environment, automatically identify tagged objects, using RF signals without direct contact, which is one of the enabling IoT technologies. In [115], it is explained a mobile RFID network based on EPC and are analyzed the threats of the mobile RFID system. Such an architecture guarantees security and efficiency.

Moreover, for the security and privacy of mobile RFID systems, another security and privacy model is proposed about IoT in [116]. The model does not only take into account the privacy of tags and readers, but also supports tags corruption, reader corruption, multiple readers and mutual authenticated key exchange protocols.

Powered by location based services, IoT systems have the potential to enable a systematic mass surveillance and to violate the personal privacy of users, especially their location privacy. [117] overviews some of the existing location privacy issues found in mobile devices. Particular attention is paid to the current access permission mechanisms used on the Android, iPhone, and Windows Mobile platforms. Note that the actual privacy issues in mobile platforms should be inherited by IoT and integrated with other static platforms.

In [118] a secure handshake scheme among mobile nodes is proposed in an intelligent transportation system. More in details, a mobile node verifies, over an insecure communication channel, the legitimacy of an ordinary sensor node by a private negotiation of the handshake attributes; in this way, a mobile hierarchy is established in order to query a deployed WSN in a secure manner.

[119] points out that secure healthcare service is a new demand for mobile solutions. To protect the privacy and security of patients in an healthcare context using an IoT infrastructure, a security and privacy mechanism is proposed. From trustworthiness point of view, service providers have to get authentication from a public authority, which is also responsible for handover cryptography credentials to each actor, in order to allow a secure communication among the end-devices and the application brokers; the goal is to establish a trusted IoT application market, where information on end-devices can be exchanged to establish a secure connection among market and users.

In [120], a security architecture deployable on mobile platforms is defined for mobile e-health applications. In particular, RFID tag identification in medical context and structured and secured IoT solutions are combined, in order to enable ubiquitous and easy access to medical related records, while providing control and security to all interactions.

Also in [116] and [121] the mobile RFID technology is exploited to solve the following security and privacy issues: not all existing tags support hash function in designing RFID protocols and channels between readers and server are not always secure in a mobile context. Therefore, a ultralightweight and privacy-preserving authentication protocol for mobile RFID systems is defined, using only bitwise XOR and several special constructed pseudo-random number generators. Such a work provides several privacy properties (e.g., tag anonymity, tag location privacy, reader privacy, mutual authentication) and avoids suffering from a number of attacks (e.g., replay attacks, desynchronization attacks).

In [122] an efficient and secure mobile-Intrusion Prevention Systems (m-IPS) is proposed for business activities using mobile devices for human-centric computing. Such a system checks user temporal and spatial information, profiles

and role information to provide precise access control.

[123] designs a mobile information collection system based on IoT, implementing an access gateway by smart mobile devices. Moreover, besides the authentication of the mobile terminals through the gateway, a key role is played by the collection strategy, which exploits the historical data movement paths, in order to reduce the problem of too long time device connection, improving the efficiency of information transmission.

In [124] special attention is paid to security and mobility in IoT. In fact, people and companies want to secure their data using firewalls, which inevitably leads to a challenging conflict between data security and usability. Since lots of products are becoming increasingly mobile, the authors of [124] design a Quantum Lifecycle Management (QLM) messaging standard in order to provide generic and standardized application-level interfaces to guarantee a two-way communications through any type of firewall, for example to perform real-time control.

A Mobile Sensor Data Processing Engine (MOSDEN) is presented in [125], which is a plug-in-based IoT middleware for resource-constrained mobile devices (until now built on Android platform), which allows to collect and process sensor data without programming efforts. It supports both push and pull data streaming mechanism as well as centralized and decentralized (e.g., peer-to-peer) data communication.

Hence, since a large number of IoT devices is likely to be mobile, a mobility management protocol is required in order to maintain IP connectivity, for example through the 6LoWPAN standard, as proposed in [126]. Other works, such as [127], deals with the efficient video dissemination in mobile multimedia IoT applications, while [128] studies the interaction of smart things with the traditional web technologies by means of a mobile Bluetooth platform. Social relationships in mobile nodes in IoT by means of a cognitive model are investigated in [129], while the use of NFC for payments with mobile devices in the so called Web of Things (WoT) is studied in [130], which proposes a lightweight architecture based on RESTful approaches.

Summarizing, also if the security issues of mobile devices (i.e., devices identification and authentication, key and credential storage and exchange) are under investigation by the scientific community, the available solutions partially address these needs, thus requiring further efforts in order to allow the integration with the other IoT technologies.

8. Ongoing Projects

Security and privacy in IoT are object of interest of European Commission. In fact, there are many projects addressing such issues in IoT field.

Butler [131] is an European Union FP7 project; its purpose is enabling the development of secure and smart life assistant applications by means of a context and location-aware, pervasive information system. It focuses on the following scenarios: smart-cities, smart-health, smart-home/smart-office, smart-shopping, smart-mobility/smart-transport. As regards security and privacy requirements, Butler project aims at allowing users to manage their distributed profile; this implies the control of data duplication and of identities sharing over distributed applications. The final purpose is to implement a framework able to integrate user dynamic data (i.e., location, behavior) in privacy and security protocols.

[132] presents an Intrusion Detection System (IDS) framework for IoT systems empowered by IPv6 over low-power personal area network (6LoWPAN) devices, which is a protocol suitable for resource constrained IoT environments. 6LoWPAN devices are vulnerable to attacks inherited from both the wireless networks and Internet protocols. The proposed IDS framework, which includes a monitoring system and a detection engine, has been integrated into the network framework developed within the EU FP7 project EBBITS [55].

The Hydra project [133] develops a middleware for Networked Embedded Systems, based on a Service-Oriented Architecture (SOA). It is co-funded by the European Commission. Hydra contemplates distributed security issues and social trust among the middleware components. Such a middleware allows de-

velopers to incorporate heterogeneous physical devices into their applications by offering easy-to-use web service interfaces for controlling any type of physical device without relying on the various network technology involved, such as Bluetooth, RF, ZigBee, RFID, WiFi, etc. Hydra incorporates means for Device and Service Discovery, Semantic Model Driven Architecture, P2P communication and Diagnostics.

The uTRUSTit (Usable Trust in the Internet of Things) [134], EU-funded FP7 project, aims at creating a trust feedback toolkit in order to enhance the user trust perception in a IoT context. uTRUSTit enables system manufacturers and system integrators to express underlying security concepts to users in a comprehensive way, allowing them to make valid judgments on the trustworthiness of such systems.

iCore project [135] provides a management framework as a wider IoT ecosystem, able to be used by different kinds of users and stakeholders and across different applications domains. The iCore proposed solution is a cognitive framework including three levels of functionality: virtual objects (VOs), composite virtual objects (CVOs), and functional blocks, for representing the user/stakeholder perspectives. Of particular importance are VOs, which are cognitive virtual representations of real-world objects (i.e., sensors, devices, everyday objects) and hide the underlying technological heterogeneity. Whereas CVOs are cognitive mashups of semantically interoperable VOs, delivering services in accordance with the user/stakeholder requirements. The difference between a real or digital object and a virtual object is that the former may be owned or controlled by a particular stakeholder, whereas the latter can be owned or controlled by particular service providers. CVOs may be owned or controlled by yet another provider who adds value by combining different virtual objects and providing these combinations to users. This leads to a hierarchical structure and therefore to a complex eco-system, which is hidden from the different stakeholders and opens new opportunities. The iCore solution shall be equipped with essential security protocols/functionalities, which span all levels of the framework and take into account the ownership and privacy of data and the access to ob-

jects. It will guarantee the secure distribution and aggregation of information exchanged among the architecture components, as well as between physical and virtual world. To test the effectiveness of such proposals, iCore addresses the following use-cases: ambient-assisted living, smart-office, smart-transportation and supply chain management.

Also beyond Europe, other countries concur with several projects to deal with security issues in IoT. In US, in 2012 DARPA announced the High Assurance Cyber Military Systems program (HACMS) [136], which is trying to patch the security vulnerabilities of IoT. The agency wants to make sure that military vehicles, medical equipment, and even drones cannot be hacked from the outside. HACMS aims at providing the seeds for future security protocols, allowing IoT to get off the ground, achieveing sufficient standardization and security. In the future, some of the software tools emerged from the HACMS program could be reverted to civil usage. Another institute interested in security in the cyber-physical systems is the National Science Foundation (NSF) [137]. Its financed Roseline project [138] aims at finding robustness solutions for cyber-physical systems to accurately and securely interact with time; in fact, the coordination of the activities within the infrastructure, the control of communications and the knowledge of time to infer location emerge critical issues for real-time security. Roseline project will be implemented across a variety of sectors, such as smart grids, aerospace systems, safety systems and autonomous vehicles. Other multi-institutional projects included in the NSF Future Internet Architectures (FIA) program, are: XIA-NP (Deployment-Driven Evaluation and Evolution of the eXpressive Internet Architecture) [139], NDN-NP (Named Data Networking Next Phase) [140], NEBULA [141], and MobilityFirst-NP (Next-Phase MobilityFirst-NP Project) [142]. They aim at exploring novel network architectures and networking concepts, such as new communications protocols, able to extend beyond current networking components, mechanisms and application requirements. They also consider the larger societal, economic and legal issues which arise from the interplay between Internet and society, providing support for mobility and enhancing the cyber-security.

More in details, XIA-NP [139] addresses the growing diversity of network models, the need for trustworthy communication, and the growing set of stakeholders who coordinate their activities to provide Internet services. XIA-NP defines the application programming interface (API) for communication and the network communication mechanisms, guaranteeing the integrity and the authentication of communication. In fact, XIA-NP enables flexible context-dependent mechanisms for establishing trust among the communicating devices. NDN-NP [140] addresses the technical challenges, including routing scalability, fast forwarding, trust models, network security, content protection and privacy. NEBULA [141] provides an architecture dealing with cloud computing; in such a project the data centers are connected by a high-speed, extremely reliable and secure backbone network, aiming at developing new trustworthy data, control and core networking approaches to support the emerging cloud computing model of always-available network services. The architecture proposed by MobilityFirst-NP [142] uses generalized delay-tolerant networking (GDTN) to provide robustness even in presence of link/network disconnections. GDNT is integrated with self-certifying public key addresses, providing a trustworthy network. Dealing with mobility, MobilityFirst-NP allows functionalities like context and location-aware services to fit naturally into the network. Such a project focuses on the tradeoffs between mobility and scalability and on opportunistic use of network resources to achieve effective communications among mobile endpoints.

Furthermore, the National Basic Research Program of China [143] raises the problem of security protection during the interaction process among the network entities, focusing on the information representation and balancing between efficiency and energy consumption. Europe collaborates both with China and Korea in the realization of an IoT architecture within the Future Internet Research and Experimentation (FIRE) project [144] [145], which aims at finding solutions for the deployment of IoT technologies in several application areas (e.g., public safety, social security, medical and health services, urban management, people livelihood) with particular attention to information security, privacy and intellectual property right. Also the EU-Japan ICT Cooperation

Table 3: Contribution of ongoing European projects on IoT security

	Butler	*EBBITS*	*Hydra*	*uTRUSTit*	*iCore*	*HACMS*	*NSF*	*FIRE*	*EUJapan*
Authentication	x			x	x	x	x	x	
Confidentiality	x	x	x		x	x	x	x	x
Access Control	x	x		x	x	x	x	x	
Privacy	x				x		x	x	x
Trust				x	x		x		
Enforcement									
Middleware		x	x		x				
Mobile	x						x		

[146] carries on a collaboration between Europe and Japan as regards the so called Future Internet; its key drivers are: the establishment of common global standards to ensure seamless communications and common ways to store and access information, the guarantee of highest security, and energy efficiency standards.

As regards worldwide projects, there are several attempts which address IoT requirements in terms of security, privacy and trust in order to develop an unified framework or middleware. In Table 3 the IoT security open issues faced by each project are summarized. At the moment the efforts are aimed at specific application contexts and the impact of these proposals on a mass-scale market still needs to be checked.

9. Conclusions

The real spreading of IoT services requires customized security and privacy levels to be guaranteed. The broad overview provided with this survey arises many open issues, and shed some light on research directions in the IoT security field. More in details, a unified vision regarding the insurance of security and privacy requirements in such an heterogeneous environment, involving different technologies and communication standards is still missing. Suitable solutions need to be designed and deployed, which are independent from the exploited platform and able to guarantee: confidentiality, access control, and privacy for users and things, trustworthiness among devices and users, compliance with

defined security and privacy policies. Research efforts are also required to face the integration of IoT and communication technologies in a secure middleware, able to cope with the defined protection constraints. Another research field is that of IoT security in mobile devices, increasingly widespread today. Much efforts have been (and are being) spent by the worldwide scientific community to address aforementioned topics, but there are still many open issues to be faced. We hope that this paper will be helpful in suggesting the research road ahead, in order to allow a massive deployment of IoT systems in real world.

References

[1] L. Atzori, A. Iera, G. Morabito, The internet of things: A survey, Comput. Netw. 54 (15) (2010) 2787–2805.

[2] 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.

[3] M. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L. Grieco, G. Boggia, M. Dohler, Standardized protocol stack for the internet of (important) things, Communications Surveys Tutorials, IEEE 15 (3) (2013) 1389–1406.

[4] B. Emmerson, M2M: the Internet of 50 billion devices, Huawei Win-Win Magazine Journal (4) (2010) 19–22.

[5] D. Boswarthick, O. Elloumi, O. Hersent, M2M Communications: A Systems Approach, 1st Edition, Wiley Publishing, 2012.

[6] O. Hersent, D. Boswarthick, O. Elloumi, The Internet of Things: Key Applications and Protocols, 2nd Edition, Wiley Publishing, 2012.

[7] L. A. Grieco, M. B. Alaya, T. Monteil, K. K. Drira, Architecting information centric ETSI-M2M systems, in: IEEE PerCom, 2014.

[8] R. H. Weber, Internet of things - new security and privacy challenges, Computer Law & Security Review 26 (1) (2010) 23–30.

[9] H. Feng, W. Fu, Study of recent development about privacy and security of the internet of things, in: 2010 International Conference on Web Information Systems and Mining (WISM), Sanya, 2010, pp. 91–95.

[10] R. Roman, J. Zhou, J. Lopez, On the features and challenges of security and privacy in distributed internet of things, Computer Networks 57 (10) (2013) 2266–2279.

[11] J. Anderson, L. Rainie, The internet of things will thrive by 2025, PewResearch Internet Project, http://www.pewinternet.org/2014/05/14/internet-of-things/, May 2014.

[12] S. Bandyopadhyay, M. Sengupta, S. Maiti, S. Dutta, A survey of middleware for internet of things, in: Third International Conferences, WiMo 2011 and CoNeCo 2011, Ankara, Turkey, 2011, pp. 288–296.

[13] M. A. Chaqfeh, N. Mohamed, Challenges in middleware solutions for the internet of things, in: 2012 International Conference on Collaboration Technologies and Systems (CTS), Denver, CO, 2012, pp. 21–26.

[14] S. Babar, A. Stango, N. Prasad, J. Sen, R. Prasad, Proposed embedded security framework for internet of things (iot), in: 2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology, Wireless VITAE 2011, Chennai, India, 2011, pp. 1 – 5.

[15] M. C. Domingo, An overview of the internet of underwater things, Journal of Network and Computer Applications 35 (6) (2012) 1879–1890.

[16] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of Things (IoT): A vision, architectural elements, and future directions, Future Generation Computer Systems 29 (7) (2013) 1645–1660.

[17] Z. Yan, P. Zhang, A. V. Vasilakos, A survey on trust management for internet of things, Journal of Network and Computer Applications 42 (0) (2014) 120–134.

[18] Y. Zhao, Research on data security technology in internet of things, in: 2013 2nd International Conference on Mechatronics and Control Engineering, ICMCE 2013, Dalian, China, 2013, pp. 1752–1755.

[19] T. Kothmayr, C. Schmitt, W. Hu, M. Brunig, G. Carle, Dtls based security and two-way authentication for the internet of things, Ad Hoc Networks 11 (8) (2013) 2710–2723.

[20] R. Roman, C. Alcaraz, J. Lopez, N. Sklavos, Key management systems for sensor networks in the context of the internet of things, Computers & Electrical Engineering 37 (2) (2011) 147–159.

[21] W. Du, J. Deng, Y. Han, P. Varshney, J. Katz, A. Khalili, A pairwise key predistribution scheme for wireless sensor networks, ACM Transactions on Information and System Security (TISSEC) 8 (2) (2005) 228–258.

[22] D. Liu, P. Ning, Establishing pairwise keys in distributed sensor networks, in: CCS '03 Proceedings of the 10th ACM conference on Computer and communications security, Washington, DC, USA, 2003, pp. 52–61.

[23] H. Pranata, R. Athauda, G. Skinner, Securing and governing access in ad-hoc networks of internet of things, in: Proceedings of the IASTED International Conference on Engineering and Applied Science, EAS 2012, Colombo, Sri Lanka, 2012, pp. 84–90.

[24] H. Ning, A security framework for the internet of things based on public key infrastructure, Advanced Materials Research 671-674 (2013) 3223–3226.

[25] Z.-Q. Wu, Y.-W. Zhou, J.-F. Ma, A security transmission model for internet of things, Jisuanji Xuebao/Chinese Journal of Computers 34 (8) (2011) 1351–1364.

[26] G. Piro, G. Boggia, L. A. Grieco, A standard compliant security framework for ieee 802.15.4 networks, in: Proc. of IEEE World Forum on Internet of Things (WF-IoT), Seoul, South Korea, 2014, pp. 27–30.

[27] I. Akyildiz, W.Su, Y.Sankarasubramaniam, E. Cayirci, A survey on sensor networks, IEEE Communications Magazine 40 (8) (2002) 102–114.

[28] H. Chan, A. Perrig, Security and privacy in sensor networks, IEEE Communications Magazine 36 (10) (2003) 103–105.

[29] J. Yick, B. Mukherjee, D. Ghosal, Wireless sensor network survey, Computer Networks 52 (12) (2008) 2292–2330.

[30] N. Li, N. Zhang, S. K. Das, B. Thuraisingham, Privacy preservation in wireless sensor networks: A state-of-the-art survey, Ad Hoc Networks 7 (8) (2009) 1501–1514.

[31] J. Zhang, V. Varadharajan, Security and privacy in sensor networks, Journal of Network and Computer Applications 33 (2) (2010) 63–75.

[32] G.Sharmam, S. Bala, A. K. Verma, Security frameworks for wireless sensor networks-review, in: 2nd International Conference on Communication, Computing & Security, ICCCS-2012, 2012, pp. 978–987.

[33] J.-Y. Lee, W.-C. Lin, Y.-H. Huang, A lightweight authentication protocol for internet of things, in: 2014 International Symposium on Next-Generation Electronics, ISNE 2014, Kwei-Shan, 2014, pp. 1–2.

[34] M. Turkanovi, B. Brumen, M. Hlbl, A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the internet of things notion, Ad Hoc Networks 20 (2014) 96–112.

[35] N. Ye, Y. Zhu, R.-C. b. Wang, R. Malekian, Q.-M. Lin, An efficient authentication and access control scheme for perception layer of internet of things, Applied Mathematics and Information Sciences 8 (4) (2014) 1617–1624.

[36] A. Alcaide, E. Palomar, J. Montero-Castillo, A. Ribagorda, Anonymous authentication for privacy-preserving iot target-driven applications, Computers & Security 37 (2013) 111–123.

[37] J. Ma, Y. Guo, J. Ma, J. Xiong, T. Zhang, A hierarchical access control scheme for perceptual layer of iot, Jisuanji Yanjiu yu Fazhan/Computer Research and Development 50 (6) (2013) 1267–1275.

[38] C. Hu, J. Zhang, Q. Wen, An identity-based personal location system with protected privacy in IoT, in: Proceedings - 2011 4th IEEE International Conference on Broadband Network and Multimedia Technology, IC-BNMT 2011, Shenzhen, China, 2011, pp. 192–195.

[39] M. Ali, M. ElTabakh, C. Nita-Rotaru, FT-RC4: A robust security mechanism for data stream systems, Tech. Rep. TR-05-024, Purdue University (November 2005).

[40] M. A. Hammad, M. J. Franklin, W. Aref, A. K. Elmagarmid, Scheduling for shared window joins over data streams, in: Proceedings of the 29th International Conference on Very Large Data Bases, VLDB '03, Berlin, Germany, 2003, pp. 297–308.

[41] S. Papadopoulos, Y. Yang, D. Papadias, Cads: continuous authentication on data streams, in: Proceedings of the 33rd International Conference on Very Large Data Bases, VLDB '07, Vienna, Austria, 2007, pp. 135–146.

[42] S. Papadopoulos, Y. Yang, D. Papadias, Continuous authentication on relational data streams, VLDB Journal 19 (1) (2010) 161–180.

[43] S. Papadopoulos, G. Cormode, A. Deligiannakis, M. Garofalakis, Lightweight authentication of linear algebraic queries on data streams, in: Proceedings of the 2013 ACM SIGMOD International Conference on Management of Data, SIGMOD '13, New York, USA, 2013, pp. 881–892.

[44] W. Lindner, J. Meier, User interactive internet of things privacy preserved access control, in: 10th International Database Engineering and Applications Symposium, 2006, IDEAS '06, Delhi, 2006, pp. 137–147.

[45] D. J. Abadi, Y. Ahmad, M. Balazinska, M. Cherniack, J. Hwang, W. Lindner, A. S. Maskey, E. Rasin, E. Ryvkina, N. Tatbul, Y. Xing, S. Zdonik, The design of the borealis stream processing engine, in: In CIDR, 2005, pp. 277–289.

[46] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, C. E. Youman, Role-based access control models, Computer 29 (2) (1996) 38–47.

[47] R. Nehme, E. Rundesteiner, E. Bertino, A security punctuation framework for enforcing access control on streaming data, in: Proceedings of the 24th International Conference on Data Engineering, ICDE '08, Cancun, Mexico, 2008, pp. 406–415.

[48] R. Nehme, E. Rundesteiner, E. Bertino, Tagging stream data for rich real-time services, Proceedings of the VLDB Endowment 2 (1) (2009) 73–84.

[49] Y. Zhu, E. A. Rundensteiner, G. T. Heineman, Dynamic plan migration for continuous queries over data streams, in: Proceedings of the ACM SIGMOD International Conference on Management of Data, SIGMOD '04, Paris, France, 2004, pp. 431–442.

[50] B. Carminati, E. Ferrari, K. L. Tan, Enforcing access control over data streams, in: Proceedings of the 12th ACM symposium on Access control models and technologies, SACMAT '07, Sophia Antipolis, France, 2007, pp. 21–30.

[51] B. Carminati, E. Ferrari, K. L. Tan, Specifying access control policies on data streams, in: Proceedings of the Database System for Advanced Applications Conference, DASFAA 2007, Bangkok, Thailand, 2007, pp. 410–421.

[52] D. J. Abadi, D. Carney, U. Cetintemel, M. Cherniack, C. Convey, S. Lee, M. Stonebraker, N. Tatbul, S. Zdonik, Aurora: a new model and architecture for data stream management, VLDB Journal 12 (2) (2003) 120–139.

[53] B. Carminati, E. Ferrari, K. L. Tan, A framework to enforce access control over data streams, ACM Trans. Inform. Syst. Sec., TISSEC 13 (3) (2010) 1–31.

[54] S. Gusmeroli, S. Piccionea, D. Rotondi, A capability-based security approach to manage access control in the internet of things, Mathematical and Computer Modelling 58 (5-6) (2013) 1189–1205.

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

[56] P. Mahalle, S. Babar, N. Prasad, R. Prasad, Identity management framework towards internet of things (IoT): Roadmap and key challenges, Communications in Computer and Information Science 89 (2010) 430–439.

[57] A. Cherkaoui, L. Bossuet, L. Seitz, G. Selander, R. Borgaonkar, New paradigms for access control in constrained environments, in: Reconfigurable and Communication-Centric Systems-on-Chip (ReCoSoC), 2014 9th International Symposium on, Montpellier, 2014, pp. 1–4.

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

[59] S. Sicari, A. Rizzardi, C. Cappiello, A. Coen-Porisini, A NFP model for internet of things applications, in: Proc. of IEEE WiMob, Larnaca, Cyprus, 2014, pp. 164–171.

[60] D. Evans, D. Eyers, Efficient data tagging for managing privacy in the internet of things, in: Proceedings - 2012 IEEE Int. Conf. on Green Computing and Communications, GreenCom 2012, Conf. on Internet of Things, iThings 2012 and Conf. on Cyber, Physical and Social Computing, CPSCom 2012, Besancon, France, 2012, pp. 244–248.

[61] X. Huang, R. Fu, B. Chen, T. Zhang, A. Roscoe, User interactive internet of things privacy preserved access control, in: 7th International Conference for Internet Technology and Secured Transactions, ICITST 2012, London, United Kingdom, 2012, pp. 597–602.

[62] J. Cao, B. Carminati, E. Ferrari, K. L. Tan, CASTLE: Continuously anonymizing data streams, IEEE Transactions on Dependable and Secure Computing 8 (3) (2011) 337–352.

[63] J. Yang, B. Fang, Security model and key technologies for the internet of things, The Journal of China Universities of Posts and Telecommunications 8 (2) (2011) 109–112.

[64] Y. Wang, Q. Wen, A privacy enhanced dns scheme for the internet of things, in: IET International Conference on Communication Technology and Application, ICCTA 2011, Beijing, China, 2011, pp. 699–702.

[65] X. Wang, J. Zhang, E. Schooler, M. Ion, Performance evaluation of attribute-based encryption: Toward data privacy in the IoT, in: 2014 IEEE International Conference on Communications, ICC 2014, Sydney, NSW, 2014, pp. 725–730.

[66] J. Su, D. Cao, B. Zhao, X. Wang, I. You, ePASS: An expressive attribute-based signature scheme with privacy and an unforgeability guarantee for the internet of things, Future Generation Computer Systems 33 (0) (2014) 11 – 18.

[67] L. b. Peng, W. b. Ru-chuan, S. Xiao-yu, C. Long, Privacy protection based on key-changed mutual authentication protocol in internet of things, Communications in Computer and Information Science 418 CCIS (2014) 345–355.

[68] A. Ukil, S. Bandyopadhyay, A. Pal, Iot-privacy: To be private or not to be private, in: Proceedings - IEEE INFOCOM, Toronto, ON, 2014, pp. 123–124.

[69] S. Sicari, C. Cappiello, F. D. Pellegrini, D. Miorandi, A. Coen-Porisini, A security-and quality-aware system architecture for internet of things, Information Systems Frontiers (2014) 1–13.

[70] F. Bao, I. Chen, Dynamic trust management for internet of things applications, in: Proceedings of the 2012 international workshop on Self-aware internet of things, Self-IoT '12, USA, San Jose, 2012, pp. 1–6.

[71] F. Bao, I. Chen, Trust management for the internet of things and its application to service composition, in: 13th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, WoWMoM 2012, San Francisco, CA, United States, 2012, pp. 1–6.

[72] M. Nitti, R. Girau, L. Atzori, A. Iera, G. Morabito, A subjective model for trustworthiness evaluation in the social internet of things, in: 2012 IEEE 23rd International Symposium on Personal Indoor and Mobile Radio Communications, PIMRC, Australia, Sydney, 2012, pp. 18–23.

[73] S. D. Kamvar, M. T. Schlosser, H. Garcia-Molina, The eigen-trust algorithm for reputation management in p2p networks, in: Proc. WWW'03, New York, USA, 2003, pp. 640–651.

[74] L. Xiong, L. Liu, Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities, IEEE Transactions on Knowledge and Data Engineering 16 (2004) 843–857.

[75] A. A. Selcuk, E. Uzun, M. R. Pariente, A reputation-based trust management system for p2p networks, in: Proc. of CCGRID 2004, Washington, DC, USA, 2004, pp. 251–258.

[76] B. Yu, M. P. Singh, K. Sycara, Developing trust in large-scale peer-to-peer systems, in: Proc. of First IEEE Symposium on Multi-Agent Security and Survivability, 2004, pp. 1–10.

[77] Z. Liang, W. Shi, Enforcing cooperative resource sharing in untrusted p2p computing environments, Mob. Netw. Appl. 10 (2005) 251–258.

[78] R. Lacuesta, G. Palacios-Navarro, C. Cetina, L. Penalver, J. Lloret, Internet of things: where to be is to trust, EURASIP Journal on Wireless Communications and Networking 2012 (1) (2012) 1–16.

[79] P. N. Mahalle, P. A. Thakre, N. R. Prasad, R. Prasad, A fuzzy approach to trust based access control in internet of things, in: 2013 3rd International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems, VITAE, NJ, Atlantic City, 2013, pp. 1–5.

[80] J.Wang, S. Bin, Y. Yu, X. Niu, Distributed trust management mechanism for the internet of things, Applied Mechanics and Materials 347-350 (4) (2013) 2463–2467.

[81] Y. Liu, Z. Chen, F. Xia, X. Lv, F. Bu, An integrated scheme based on service classification in pervasive mobile services, International Journal of Communication Systems 25 (9) (2012) 1178–1188.

[82] Y. Liu, Z. Chen, F. Xia, X. Lv, F. Bu, A trust model based on service classification in mobile services, in: Proceedings - 2010 IEEE/ACM International Conference on Green Computing and Communications, GreenCom 2010, 2010 IEEE/ACM International Conference on Cyber, Physical and Social Computing, CPSCom 2010, Hangzhou, China, 2010, pp. 572–576.

[83] L. Wen-Mao, Y. Li-Hua, F. Bin-Xing, Z. Hong-Li, A hierarchical trust model for the internet of things, Chinese Journal of Computers 5 (2012) 846–855.

[84] Y. Saied, A. Olivereau, D. Zeghlache, M. Laurent, Trust management system design for the internet of things: A context-aware and multi-service approach, Computers & Security 39 (2013) 351–365.

[85] P. Dong, J. Guan, X. Xue, H. Wang, Attack-resistant trust management model based on beta function for distributed routing in internet of things, China Communications 9 (4) (2012) 89–98.

[86] T. Liu, Y. Guan, Y. Yan, L. Liu, Q. Deng, A wsn-oriented key agreement protocol in internet of things, in: 3rd International Conference on Frontiers of Manufacturing Science and Measuring Technology, ICFMM 2013, LiJiang, China, 2012, pp. 1792–1795.

[87] P. Martinez-Julia, A. F. Skarmeta, Beyond the separation of identifier and locator: Building an identity-based overlay network architecture for the future internet, Computer Networks 57 (10) (2013) 2280–2300.

[88] G. D. Tormo, F. G. Marmol, G. M. Perez, Dynamic and flexible selection of a reputation mechanism for heterogeneous environments, Future Generation Computer Systems (0) (2014) –.

[89] L. Gu, J. Wang, B. b. Sun, Trust management mechanism for internet of things, China Communications 11 (2) (2014) 148–156.

[90] Y.-B. Liu, X.-H. Gong, Y.-F. Feng, Trust system based on node behavior detection in internet of things, Tongxin Xuebao/Journal on Communications 35 (5) (2014) 8–15.

[91] R. Macfarlane, W. Buchanan, E. Ekonomou, O. Uthmani, L. Fan, O. Lo, Formal security policy implementations in network firewalls, Computers & Security 31 (2) (2012) 253–270.

[92] Y. Elrakaiby, F. Cuppens, N.Cuppens-Boulahia, Formal enforcement and management of obligation policies, Data & Knowledge Engineering 71 (1) (2012) 127–147.

[93] Z. Wu, L. Wang, An innovative simulation environment for cross-domain policy enforcement, Simulation Modelling Practice and Theory 19 (7) (2011) 1558–1583.

[94] M. Dell'Amico, M. S. I. G. Serme, A. S. de Oliveira, Y. Roudier, Hipolds: A hierarchical security policy language for distributed systems, Information Security Technical Report 17 (3) (2013) 81–92.

[95] G. Bella, R. Giustolisi, S. Riccobene, Enforcing privacy in e-commerce by balancing anonymity and trust, Computers & Security 30 (8) (2011) 705–718.

[96] M. Langar, M. Mejri, K. Adi, Formal enforcement of security policies on concurrent systems, Journal of Symbolic Computation 46 (9) (2011) 997–1016.

[97] J. Baeten, A brief history of process algebra, Theoret. Comput. Sci. 335 (2-3) (2005) 131–146.

[98] D. Ferraiolo, V. A. ans S. Gavrila, The policy machine: A novel architecture and framework for access control policy specification and enforcement, Journal of Systems Architecture 57 (4) (2011) 412–424.

[99] D. Brewer, M. Nash, The chinese wall security policy, in: Proceedings., 1989 IEEE Symposium on Security and Privacy, Oakland, CA, 1989, pp. 206–214.

[100] M. Bishop, Computer Security: Art and Science, Addison Wesley, 2003.

[101] J. Rao, A. Sardinha, N. Sadeh, A meta-control architecture for orchestrating policy enforcement across heterogeneous information sources, Web Semantics: Science, Services and Agents on the World Wide Web 7 (1) (2009) 40–56.

[102] J. Singh, J. Bacon, D. Eyers, Policy enforcement within emerging distributed, event-based systems, in: DEBS 2014 - Proceedings of the 8th ACM International Conference on Distributed Event-Based Systems, 2014, pp. 246–255.

[103] R. Neisse, G. Steri, G. Baldini, Enforcement of security policy rules for the internet of things, in: Proc. of IEEE WiMob, Larnaca, Cyprus, 2014, pp. 120–127.

[104] I. Bagci, S. Raza, T. Chung, U. Roedig, T. Voigt, Combined secure storage and communication for the internet of things, in: 2013 IEEE International Conference on Sensing, Communications and Networking, SECON 2013, New Orleans, LA, United States, 2013, pp. 523–631.

[105] D. Conzon, T. Bolognesi, P. Brizzi, A. Lotito, R. Tomasi, M. Spirito, The virtus middleware: An xmpp based architecture for secure IoT communications, in: 2012 21st International Conference on Computer Communications and Networks, ICCCN 2012, Munich, Germany, 2012, pp. 1–6.

[106] A. Gòmez-Goiri, P. Orduna, J. Diego, D. L. de Ipina, Otsopack: Lightweight semantic framework for interoperable ambient intelligence applications, Computers in Human Behavior 30 (2014) 460–467.

[107] M. Isa, N. Mohamed, H. H. S. Adnan, J. Manan, R. Mahmod, A lightweight and secure TFTP protocol for smart environment, in: ISCAIE 2012 - 2012 IEEE Symposium on Computer Applications and Industrial Electronics 2012, Kota Kinabalu, Malaysia, 2012, pp. 302–306.

[108] C. H. Liu, B. Yang, T. Liu, Efficient naming, addressing and profile services in internet-of-things sensory environments, Ad Hoc Networks 18 (0) (2013) 85–101.

[109] oneM2M, http://www.onem2m.org/.

[110] G. Colistra, V. Pilloni, L. Atzori, The problem of task allocation in the internet of things and the consensus-based approach, Computer Networks 73 (0) (2014) 98–111.

[111] Y. Wang, M. Qiao, H. Tang, H. Pei, Middleware development method for internet of things, Liaoning Gongcheng Jishu Daxue Xuebao (Ziran Kexue Ban)/Journal of Liaoning Technical University (Natural Science Edition) 33 (5) (2014) 675–678.

[112] H. Ferreira, R. De Sousa Jr., F. De Deus, E. Canedo, Proposal of a secure, deployable and transparent middleware for internet of things, in: Iberian

Conference on Information Systems and Technologies, CISTI, Barcelona, 2014, pp. 1–4.

[113] J. Mao, L. Wang, Rapid identification authentication protocol for mobile nodes in internet of things with privacy protection, Journal of Networks 7 (7) (2012) 1099–1105.

[114] A. Jara, V. Kafle, A. Skarmeta, Secure and scalable mobility management scheme for the internet of things integration in the future internet architecture, International Journal of Ad Hoc and Ubiquitous Computing 13 (3-4) (2013) 228–242.

[115] T. Yan, Q. Wen, A secure mobile rfid architecture for the internet of things, in: Proceedings 2010 IEEE International Conference on Information Theory and Information Security, ICITIS 2010, Beijing, China, 2010, pp. 616–619.

[116] W. Zhu, J. Yu, T. Wang, A security and privacy model for mobile rfid systems in the internet of things, in: International Conference on Communication Technology Proceedings, ICCT, 2012, pp. 726–732.

[117] M. Elkhodr, S. Shanhrestani, H. Cheung, A review of mobile location privacy in the internet of things, in: International Conference on ICT and Knowledge Engineering, Bangkok, Thailand, 2012, pp. 266–272.

[118] S. Li, P. Gong, Q. Yang, M. Li, J. Kong, P. Li, A secure handshake scheme for mobile-hierarchy city intelligent transportation system, in: International Conference on Ubiquitous and Future Networks, ICUFN, Da Nang, 2013, pp. 190–191.

[119] K. c. Kang, Z.-B. Pang, C. c. Wang, Security and privacy mechanism for health internet of things, Journal of China Universities of Posts and Telecommunications 20 (SUPPL-2) (2013) 64–68.

[120] F. Goncalves, J. Macedo, M. Nicolau, A. Santos, Security architecture for mobile e-health applications in medication control, in: 2013 21st In-

ternational Conference on Software, Telecommunications and Computer Networks, SoftCOM 2013, Primosten, 2013, pp. 1–8.

[121] B. Niu, X. Zhu, H. Chi, H. Li, Privacy and authentication protocol for mobile rfid systems, Wireless Personal Communications 77 (3) (2014) 1713–1731.

[122] Y.-S. Jeong, J. Lee, J.-B. Lee, J.-J. Jung, J. Park, An efficient and secure m-ips scheme of mobile devices for human-centric computing, Journal of Applied Mathematics Special Issue 2014 (2014) 1–8.

[123] J. Geng, X. Xiong, Research on mobile information access based on internet of things, Applied Mechanics and Materials 539 (2014) 460–463.

[124] S. Kubler, K. Frmling, A. Buda, A standardized approach to deal with firewall and mobility policies in the iot, Pervasive and Mobile Computing (0) (2014) –.

[125] C. Perera, P. Jayaraman, A. Zaslavsky, D. Georgakopoulos, P. Christen, Mosden: An internet of things middleware for resource constrained mobile devices, in: Proceedings of the Annual Hawaii International Conference on System Sciences, Washington, DC, USA, 2014, pp. 1053–1062.

[126] J. Montavont, D. Roth, T. Nol, Mobile {IPv6} in internet of things: Analysis, experimentations and optimizations, Ad Hoc Networks 14 (0) (2014) 15–25.

[127] D. Rosario, Z. Zhao, A. Santos, T. Braun, E. Cerqueira, A beaconless opportunistic routing based on a cross-layer approach for efficient video dissemination in mobile multimedia IoT applications, Computer Communications 45 (0) (2014) 21–31.

[128] J. P. Espada, V. G. Díaz, R. G. Crespo, O. S. Martínez, B. P. G-Bustelo, J. M. C. Lovelle, Using extended web technologies to develop bluetooth multi-platform mobile applications for interact with smart things, Information Fusion 21 (0) (2015) 30–41.

[129] J. An, X. Gui, W. Zhang, J. Jiang, J. Yang, Research on social relations cognitive model of mobile nodes in internet of things, Journal of Network and Computer Applications 36 (2) (2013) 799–810.

[130] T.-M. Gronli, P. Pourghomi, G. Ghinea, Towards NFC payments using a lightweight architecture for the web of things, Computing (2014).

[131] BUTLER project, http://www.iot-butler.eu.

[132] P. Kasinathan, G. Costamagna, H. Khaleel, C. Pastrone, M. Spirito, Demo: An ids framework for internet of things empowered by 6lowpan, Berlin, Germany, 2013, pp. 1337–1339.

[133] HYDRA project, http://www.hydramiddleware.eu/.

[134] Usable trust in the internet of things, http://www.utrustit.eu/.

[135] iCORE project, http://www.iot-icore.eu.

[136] HACMS project, http://www.defenseone.com/technology.

[137] National Science Foundation project, http://www.nsf.gov.

[138] Roseline project, https://sites.google.com/site/roselineproject/.

[139] XIA-NP project, http://www.cs.cmu.edu/ xia/.

[140] NDN-NP project, http://named-data.net/.

[141] NEBULA project, http://nebula-fia.org/.

[142] MobilityFirst-NP project, http://mobilityfirst.winlab.rutgers.edu/.

[143] H.-D. Ma, Internet of things: Objectives and scientific challenges, Journal of Computer Science and Technology 26 (6) (2011) 919–924.

[144] FIRE EU-China project, http://www.euchina-fire.eu/.

[145] FIRE EU-Korea project, http://eukorea-fire.eu/.

[146] EU-Japan project, http://www.eurojapan-ict.org/.