On the Security Aspects of Internet of Things: A Systematic Literature Review

Evandro L. C. Macedo, Egberto A. R. de Oliveira, Fabio H. Silva, Rui R. Mello Jr, Felipe M. G. França, Flavia C. Delicato, José F. de Rezende, and Luís F. M. de Moraes

Abstract: **Internet of Things (IoT) has gained increasing visibility among emerging technologies and undoubtedly changing our daily life. Its adoption is strengthened by the growth of connected devices (things) as shown in recent statistics. However, as the number of connected things grows, responsibility related to security aspects also needs to increase. For instance, cyberattacks might happen if simple authentication mechanisms are not implemented on IoT applications, or if access control mechanisms are weakly defined. Considering the relevance of the subject, we performed a systematic literature review (SLR) to identify and synthesize security issues in IoT discussed in scientific papers published within a period of 8 years. Our literature review focused on four main security aspects, namely authentication, access control, data protection, and trust. We believe that a study considering these topics has the potential to reveal important opportunities and trends related to IoT security. In particular, we aim to identify open issues and technological trends that might guide future studies in this field, thus providing useful material both to researchers and to managers and developers of IoT systems. In this paper, we describe the protocol adopted to perform the SLR and present the state-of-the-art on the field by describing the main techniques reported in the retrieved studies. To the best of our knowledge, ours is the first study to compile information on a comprehensive set of security aspects in IoT. Moreover, we discuss the placement, in terms of architectural tiers, for deploying security techniques, in an attempt to provide guidelines to help design decisions of security solution developers. We summarize our results showing security trends and research gaps that can be explored in future studies.**

Index Terms: **Access control, architecture, authentication, data protection, internet of things, IoT, security, techniques, trust.**

I. INTRODUCTION

INTERNET of Things (IoT) [1] is a disruptive paradigm that brings the next wave of evolution of the Internet by extending communication among any kind of smart object (*thing*), and enabling the integration of heterogeneous technologies. As a consequence, IoT leads to the development of novel applications, as well as the improvement of existing ones, enabling unprecedented data collection.

With 29 billion of connected things estimated by 2022 [2], the spread of IoT paves the way to a myriad of applications that can improve life quality of our society. Considerable benefits can be seized, for instance, in healthcare, smart cities, smart home applications and intelligent transport systems (ITS). All these applications avail improvements due to the increased amount of data that can be obtained from things, which helps decision making processes. However, all these benefits come together with the responsibility of providing them in a secure way. If any of these systems are compromised, not only financial issues could happen. For example, in a healthcare IoT application, a tampered sensor may expose private data or deliver wrong measures of heart rate leading to prescription errors; or in an ITS if traffic lights control are hacked, this may cause the occurrence of a car crash. Thus, in this context, besides financial loss, a security flaw can lead to violation of data privacy and, in the worst cases, it may even incur physical damage to human beings. On the one hand, having connectivity at anytime for anything and anywhere is tempting and brings many advantages, but on the other hand, new requirements and challenges arise that need to be considered in the design of IoT systems and applications. According to the authors in [3]–[6], security issues, such as privacy, authorization, verification, access control, information storage, and management, are major challenges in an IoT environment. As we will discuss in Section I.A, many of the characteristics inherent to the IoT environment, such as the large scale, dynamism, and heterogeneity of devices, contribute to making such security aspects challenging. Addressing these challenges and providing suitable security solutions is essential for the development and widespread dissemination of the IoT paradigm.

A. Security Challenges in IoT

IoT, as an ecosystem composed of the merging of heterogeneous network technologies, not only inherits the same security problems from traditional wired networks, wireless networks, mobile networks, and sensor networks, but also incorporates new issues derived from its very specific characteristics.

Let's begin our discussion by the sensor devices in charge of the acquisition and monitoring of environmental variables, and major responsible for the integration between the physical and virtual worlds. Sensors nodes have limited computing and storage capacities, which prevent the implementation of robust and complex security mechanisms, for example for authentication

Manuscript received March 4, 2018; approved for publication by Naït-Abdesselam Farid, Division SI.

This study was partially funded by Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), under grant 307378/2014-4 and by Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP) under the grant 2015/24144-7 for Flavia C. Delicato, by CNPq under grant 312357/2017-6 for Jose F. de Rezende and under 309781/2016-7 for Felipe M. G. França, by Fundação de Amparo à Pesquisa do Estado do Rio de Janeiro (FAPERJ) and RedeRio (the state academic backbone network) under the grant 150.134/2010 for Luís F. M de Moraes, and in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Finance Code 001.

The authors are with the Computer Engineering and Systems Program, Federal University of Rio de Janeiro, email: {evandro, moraes}@ravel.ufrj.br, {egberto, fabhenr, ruirodrigues, felipe}@cos.ufrj.br, fdelicato@dcc.ufrj.br, jfrezende@gmail.com.

Evandro L. C. Macedo is the corresponding author.

Digital Object Identifier: 10.1109/JCN.2019.000048

purposes. It is necessary to implement lightweight technologies in the devices, which generally do not provide the highest degrees of protection. Another characteristic related to IoT devices is their heterogeneity, pervasiveness, and potential mobility. Since literally any physical object can be instrumented and become part of the IoT, there is a large increase in the attack surface. Appliances, home utilities, day-to-day objects that were not designed with security issues in mind, by being networked are now posing vulnerabilities to be exploited by malicious users. Besides, for identification and access control purposes, it is quite difficult to manage identities considering such a myriad of (potentially mobile) devices. Regarding the trust aspect, it is challenging to rely on devices that can be easily tampered since they might be mobile.

At the network layer, IoT ecosystems suffer from the same vulnerabilities of wireless networks in general, aggravated by its high dynamism, the need to integrate different technologies and the lack of standards currently in use. There is as yet no dominant technology nor a stack of standardized protocols for use in IoT. This has often led to the adoption of proprietary protocols and the creation of *ad hoc* network architectures, not always focused on providing security solutions at all layers, which can result in vulnerabilities to be exploited in cyberattacks.

The heterogeneity of IoT applications and their nature impose additional security challenges. Many applications require the acquisition of sensitive data, such as personal data (including body variables, activities and location) or industrial process monitoring data. The need to protect the data trafficked in IoT is crucial. Besides that, different IoT application fields have different industry standards and related security specifications. This makes it difficult to adopt unique and integrated security frameworks, leading to the need for customized solutions.

Finally, considering the intrinsic features of this emerging type of ecosystem constituted by IoT, it is common the occurrence of opportunistic, *ad hoc* interactions among devices and users, leveraged by some specific contexts. For instance, a mobile device can make its resources available only for users that are in its neighborhood for a given period of time. Therefore, there is a trend of adopting more relaxed business models, instead of formal contracts between parties. In this context, trust in the participating parties is a key issue and the *ad hoc* nature of interactions makes the establishment of trust a challenging aspect. In addition, the need arises to deal with the context (temporal, geo-spatial, among others) of the interactions that occur in the system. Security solutions should therefore ideally be context-aware and incorporate context information into decisions, for example, regarding authentication and access control.

B. Context and Goal of this Study

Given the relevance of the subject, many references in the current literature [3]–[5], [7]–[13] present studies that highlight the importance of considering security aspects during the development of IoT solutions, from different perspectives. In [7], the authors analyze the most relevant available solutions for security aspects such as access control, privacy, trust, confidentiality, authentication, among others. For each considered aspect, they focus on proposals that address security solutions and security middleware applied to mobile devices. They also present ongoing projects from the European Commission that address such issues in the IoT field. The authors in [3] provide an overview of IoT focusing on enabling technologies, protocols, and application issues, and highlight security as one of the main challenges that must be addressed in IoT. Alaba *et al.* [9] focus on the state-of-the-art of IoT security threats and vulnerabilities, offering a taxonomy of threats and discussing possible cyberattacks. Authors in [11] review eight IoT frameworks commercially available, pointing out the security features of the respective architectures. Khan *et al.* [12] explore open challenges on IoT security, presenting a taxonomy of security issues, focusing on blockchain-based solutions. Sfar *et al.* [13] present a roadmap of security in the IoT through a systemic and cognitive approach. By cognitive, the authors mean that their approach provides complex and dynamical interactions between process, people, technology and organization, in order to give the flexibility for the system to be able to analyze different situations and perform the most suitable measures to guarantee reliability and security. They also show related surveys that cover different security aspects (authentication, access control, privacy, confidentiality, trust, data protection, availability etc), each one with a different focus. Irshad [14] presents a study with focus on information security management frameworks for IoT, and in [5] the authors discuss about security problems in IoT considering their characteristics concerning the application layer (e.g., data protection, software vulnerabilities), network layer (e.g., DoS attacks, network congestion, authentication), and perception layer (e.g., replay attack, fake node). They also point out security measures to deal with these problems. Finally, in [4] the authors provide a survey in which secure communication protocols based on IP are explored in the IoT context. In particular, the authors discuss the applicability and limitations of existing IP-based Internet security protocols, as well as other types of security protocols used in wireless sensor networks. Such analysis is based on a taxonomy focusing on key establishment mechanisms in the context of the IoT.

However, these studies focus on specific approaches to cover security issues in IoT and do not provide a holistic view of essential aspects to provide security at different levels for these systems. Our study discusses the following security aspects: (i) Authentication; (ii) access control; (iii) data protection; and (iv) trust. We consider them as very comprehensive and encompassing further aspects. For instance, data protection includes privacy, trust includes availability, etc. Moreover, existing studies do not discuss architectural aspects in terms of the places of implementation of the security techniques. With the analysis and synthesis of the studies retrieved in our literature search, we aim to shed light on techniques that are used as security solutions and discuss where the reported techniques were implemented in terms of the architectural stack of IoT systems. We believe that the type of overview and discussions provided in our paper may help researchers to envision opportunities and reflect on the state-of-the-art to identify important challenges and research gaps regarding security in IoT. In addition, the discussion about architectural aspects may allow to scale security solutions according to restricted computational resources of IoT devices, thus helping developers of IoT systems. Among prior studies, different research methodologies were used to conduct the re-

view of the literature. One of the methodologies commonly used due to its capability of providing a set of well-defined, reproducible, and auditable steps, is the systematic literature review (SLR) [15], which comprises a research protocol that can be used in other studies. The motivation to use SLRs as an investigation method should start from real problems detected in the industrial practice, as it is the case of IoT security. The results of SLRs should, in turn, affect and improve this practice.

In our study we adopt the SLR methodology. An SLR is defined as a secondary study that applies a well-defined approach to determine, evaluate and interpret scientific evidence related to a specific research question, in a way that is unbiased and repeatable. In short, in this paper we present a comprehensive study with the following differentials and main contributions:

- We adopt a well-defined research protocol based on the SLR methodology that can be replicated and verifiable;
- We present a comprehensive review on the state of the art regarding four major security aspects;
- We discuss the location, in terms of architectural tiers, of security techniques implementations, thus providing hints that can help developers to visualize which tier(s) would be the best place to implement a specific security technique.

We believe that a study considering these topics is relevant and has the potential to reveal opportunities and trends related to IoT security. In particular, we aim to identify open issues and technological trends that might guide future studies in this area, thus providing useful material both to researchers as well as to managers and developers of IoT systems.

The rest of this article is organized as follows. Section II describes the steps and protocol adopted for the SLR execution. In Section III we present some statistics for selected studies. The analysis of each security aspects is presented in Section IV, followed by the discussion of the results, in the Section V. Finally, we conclude the paper in Section VI.

II. RESEARCH METHODOLOGY

In this section we present the methodology used to conduct the literature search and the selection of the studies to be included in our analysis. An SLR is based on the choice and subsequent analysis of a series of scientific articles, according to a well-defined protocol, so that the results can be reproduced, verified, and audited. An SLR is basically composed of three phases [16], namely: (i) Planning; (ii) Conducting the review; and (iii) reporting (Documenting) the review. Activities of defining the research questions, developing a review protocol and validating the review protocol are carried out during the Planning phase. The Conducting phase comprises identifying relevant study, selecting primary studies, assessing study quality, extracting required data, and synthesizing data. In the last phase, Documenting, researchers write a review report and validate it. According to [17] such approach has the benefits of providing an overview of a specific domain, identifying the state-of-the-art on the researched field, which is interesting for researchers who need a first approach on a particular subject. In addition, this kind of study enables the identification of research trends, raising the most discussed aspects and open issues, indicating possibilities of research in less discussed aspects.

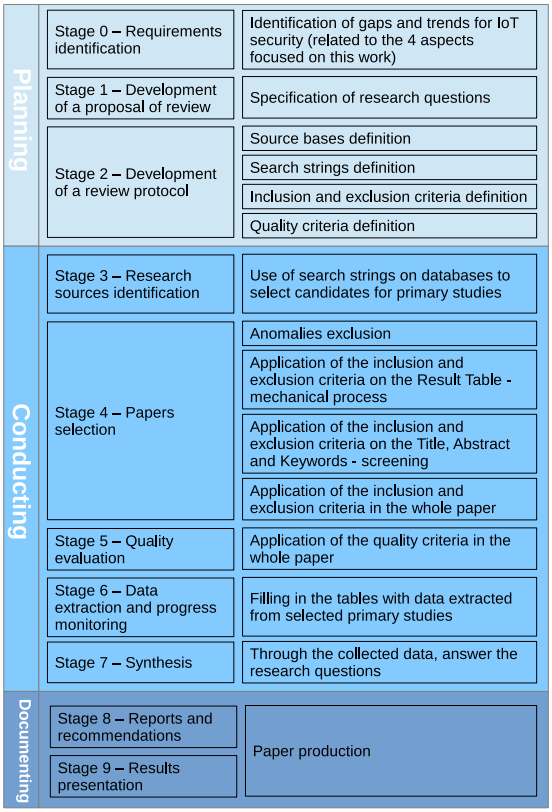


Fig. 1. Phases and stages of an SLR.

In Fig. 1 we present all phases and respective stages that compose the SLR process. The Planning phase corresponds to the set of tasks related to designing and preparing the protocol. The Conducting phase refers to the tasks that will apply the protocol until the primary studies are selected. Finally, at the Documenting phase the SLR will be produced in a paper or report format.

A. Planning

In this section we will discourse the tasks performed at the Planning phase of our SLR. This way, all the activities executed to prepare our protocol will be described below.

A.1 Requirements Identification and Research Questions

The first step to perform an SLR is the recognition of the need of performing the study, which corresponds to *Stage 0* of an SLR, according to Fig. 1. In our case, this task was accomplished by identifying the needs to uncover gaps and trends related to the four IoT security aspects addressed in this study. Therefore, it is necessary to identify some research questions (RQ) to be answered from the inputs provided by the analysis of relevant studies, which will constitute the primary studies. Specifying this RQs corresponds to the *Stage 1* of the SLR protocol.

For the specific case of our SLR, based on recent researches [18] in the field of authentication, access control, data protection, and trust applied to the IoT, the following RQs, and their respective goals have been defined, as listed in Table 1.

Table 1. Research question.

	Research questions	Goals
RQ1	What are the main security techniques that consider data protection, access control, authentication, and trust in IoT?	To obtain an overview of access control, authentication, data protection and trust techniques already proposed.
RQ2	What are the trends and gaps concerning authentication, access control, data protection, and trust?	To identify trends and gaps among considered security aspects.

A.2 Source Bases and Search Strings

According to Fig. 1, the *Stage 2* of an SLR corresponds to the definition of: Source bases, search strings, inclusion and exclusion criteria, and quality criteria. In this section, we will see details about source bases and search strings definition.

As a way to identify the primary studies necessary to our study, four scientific databases were used, namely *IEEExplore*, *Scopus*, *Science Direct*, and *Web of Science*. These electronic databases consist of some of the most relevant digital libraries for scientific studies in the area of Computer Science.

It is important to explain that the ACM Digital Library (https://dl.acm.org), another well-known source of relevant scientific information in the field, was also initially considered. Nevertheless, the absence of the Abstract field on the search results export template became an issue to the adopted review protocol as it would preclude applying the inclusion and exclusion criteria detailed ahead. Regardless, since search results are frequently repeated between different platforms, we consider removing ACM Digital Library from the group of source bases does not cause a material loss in the final outcome of our study.

As previously mentioned, one of the characteristics of an SLR is to allow the proposed process to be reproduced. For that, search strings were used to select primary studies. This search strings are specific to each library, as listed below:

- **IEEE Xplore, Science Direct, and Scopus:**
(internet of things OR internet-of-things OR iot OR web of things OR wot) AND (access control OR identity OR authentication OR data protection OR data security) AND (trust OR trust-based OR architecture OR framework)

- **Web of Science:**
TI=(internet of things OR internet-of-things OR iot OR web of things OR wot) AND TS=(access control OR identity OR authentication OR data protection OR data security) AND TS=(trust OR trust-based OR architecture OR framework)

It is important to say that due to the specificity of each digital library, the strings have some differences. However, the adequacy of each string to its respective library can be considered an important step in the process of performing an SLR, due to its ability to obtain suitable and relevant primary studies.

A.3 Inclusion and Exclusion Criteria

Once the initial choice of studies from the search in the databases is done, the next steps are to screen the retrieved studies and select the relevant ones that will be the focus of a more in depth analysis. According to the SLR methodology, described in [19], it is necessary to establish rules for selecting the relevant studies, specifically, we must define a set of inclusion/exclusion criteria. The rationale behind the adopted criteria is to select studies to be included in the literature review only if they present a scientific contribution to the body of knowledge on security aspect in IoT context. For this present paper, the following criteria were identified for inclusion and exclusion of studies, as presented in Tables 2 and 3, respectively.

Regarding the exclusion criteria, a filter was created, called "Relevance Criterion", which aims to verify the relevance of a selected study, from the point of view of the number of existing citations. The motivation behind the definition of this criterion was that we consider that studies without a minimum number of citations have little impact and have no relevant scientific potential. This filter consists of papers having at least one citation per year (considering the period from 2010 to 2016). For example, an article published in 2015 should have at least 4 citations. For articles published in 2017 or 2018 this filter was not applied, since they are considered quite recent.

As it can be seen in Table 3, some criteria aim to discard studies not related to the subject of our study, for instance, $EC1$, $EC2$ and $EC3$. Our goal is to find primary studies that can be useful to help answering the formulated research questions. Considering this, we propose the $EC11$ to remove surveys from the results of queries, as this type of publication is not considered a primary study. The last exclusion criteria, $EC12$, aims to discard studies that do not suggest any solution or new technique that can be applied on any of the four aspects focused on this paper. Finally, it is important to point out that many of these exclusion criteria are commonly used in SLR. In this sense our criteria was inspired in [17] and [20].

A.4 Quality Criteria

After applying the criteria for selection of studies described in Section II.A.3, an optional step is to filter the selected studies by some quality criteria. According to Wohlin *et al.* [21], there is no universally agreed-on and applicable definition of study quality, although the most practical means for quality assessments are checklists. For this purpose, the authors used Kitchenham *et al.* [19] guidelines as inspiration to define our quality criteria:

- *QC1* - Is there a clear statement of the aims of the research?
- *QC2* - Is the proposed architecture/algorithm/protocol feasible (it has been or can be applied to a real scenario)?
- *QC3* - Were the experiments fully/properly analyzed and explained? Does the results support the ideas shown in the paper?

According to [19], the importance of these criteria is to provide more detailed inclusion/exclusion criteria than the general ones, to weight the relevance of individual studies after synthesizing, to emphasize the differences between studies, and to guide for further research. This way, it is possible to minimize bias and maximize validity of the studies.

Still according to [19], the quality criteria of an SLR may

Table 2. Inclusion criteria.

Inclusion criteria	
$IC1$	The study presents or discusses opportunities, challenges, or schemes related to authentication, access control, data protection or trust in IoT
$IC2$	The study presents or discusses security architectures related to authentication, access control, data protection or trust in IoT

Table 3. Exclusion criteria.

Exclusion criteria	
$EC1$	The study is not related to IoT
$EC2$	The study is not related to security in IoT
$EC3$	The study does not address authentication, access control, data protection or trust in IoT
$EC4$	The study is a previous version of a more complete study about the same research subject
$EC5$	The study does not have an abstract or the full text is not available
$EC6$	The study is not written in English, which is the most common language in scientific papers
$EC7$	The study was published before 2010
$EC8$	The study consists of a book chapter
$EC9$	The study was not approved by the "Relevance Criterion"
$EC10$	The study does not present references
$EC11$	The study is a survey
$EC12$	The study does not present a proposal for solution

need to consider a measurement scale for each item, instead of a simple Yes/No answer, since it sometimes can be misleading. Hence, for each quality criterion above, it is only possible to admit one of the following three answers: “yes”, “no”, and “partially”. Each “yes” answer equals 1.0 point; 0.5 point for each “partially” answer and 0.0 for “no” answers. Finally, articles that do not sum 2.0 or more points are excluded by the quality criteria shown in (1).

$$PQC1 + PQC2 + PQC3 >= 2.0 \quad (1)$$

The PQC**n** corresponds to the score of a quality criteria of number n. The values stipulated for each quality criterion aim to assign equal weights for each one, so that the paper has to reach at least 66% of this criteria, similar to [20]. It‘s important to notice that papers excluded by these quality criteria are not considered poor quality papers, but rather it does not meet the requirements defined for our specific research goals.

So, with the definition of the source base and search strings (Section II.A.2), inclusion and exclusion criteria (Section II.A.3) and quality criteria used (Section II.A.4), we finished the *Stage 2* and the Planning phase.

B. Conducting

In this section we present more details about the application of the previously described protocol. The following stages will be detailed: Identification of research sources, paper selection, quality evaluation, data extraction and synthesis.

B.1 Steps of the Selection Process and Quality Evaluation

To accomplish our goals, four people (Ph.D. students, co-authors of this manuscript) executed the defined protocol during a time-frame of approximately five months. After defining research questions and elaborating the search strings for each source database, the searches were performed resulting in 1186 scientific papers representing candidates for primary studies. This corresponds to the *Stage 3* of the SLR, according to Fig. 1. We extracted meta-data of these studies and inserted them into a results table, to be used during the application of inclusion, exclusion, and quality criteria. The fields in the results table are described below:

- Database, Author, Title, Journal, Pages, Year, Keywords, Citations, URL, Booktitle, Abstract, Publisher, and DOI.

Once the results table is created, the *Stage 4* of the SLR can be performed. In Fig. 2, the Stages 4 (paper selection) and 5 (quality evaluation) of an SLR are shown, where we can see the number of papers excluded in each step. Note that this figure is divided into three different steps. The first step (from 1186 to 501 papers) was more “mechanical” than the others and was developed by all of the four researchers at the same time, in a sequential way, without division of the work. In the second step (from 501 to 223 papers), the papers were distributed to the researchers, who performed their work in parallel. In this step the inclusion and exclusion criteria were applied on the title, abstract and keywords (Screening). Lastly, in the step 3 of the paper selection process (from 223 to 131), the 223 papers were distributed again to the researchers. However, in this step we applied the inclusion, exclusion and quality criteria looking at the full paper. More details about these steps presented at the Fig. 2 will be described below.

- **Step 1:** The first task concerning the exclusion/filtering of papers consists in removing from the results table the records that presented “anomalies” returned by the search. For example, records that returned inconsistency on some fields, such as publications missing author names, abstract or title. Thus, we removed 25 search anomalies. Another important step in this stage was removing duplicated papers from this initial table. We found that 115 papers were duplicated. So, we have reached a total of 1046 pre-selected articles. After this initial removal of papers, we applied the defined inclusion and exclusion criteria at the fields of the results table, in a “mechanical” way. This means that we use some formulas, macros and other tools to fil-

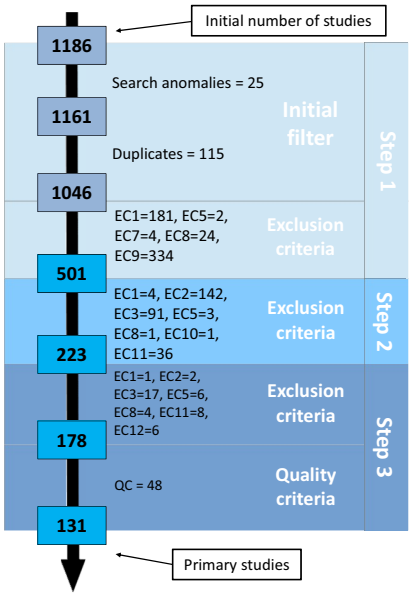


Fig. 2. Number of papers excluded per step.

ter the fields of the result table searching for papers that would be removed without a detailed analysis. For instance, the relevance criterion (defined at the Section II.A.3) was applied on the records of the result table through a formula in the worksheet. This way, after applying the inclusion and exclusion criteria through this mechanical process, we reached a number of 501 pre-selected papers. It's very important to mention that all tasks described at the step 1 of the Fig. 2 were applied by all of the four researchers together, without distribution of the work. The intention was to reach a common understanding and felling about the application of the protocol by each researcher and decrease potential biases.

- **Step 2:** Resuming the selection process to identify the primary studies, the 501 articles selected in the previous phase were distributed between the four researches. Thus, the step two of our selection process consists of applying the exclusion criteria in the abstract, title, and keywords (screening), reaching a total of 223 selected articles. So, until the present step, it was not necessary reading the whole paper.
- **Step 3:** The 223 selected articles in step two were divided among the researchers once again, totaling about 56 articles per researcher. In this step, the papers were fully analyzed by means of their complete reading. After this more detailed analysis, from the initial set of 223 articles, 45 were eliminated by exclusion criteria. The studies were evaluated from the perspective of the quality criteria (described in Section II.A.4) in which 48 articles were removed of our analysis. Thus, after performing all the steps responsible for the elimination of articles, 131 primary studies were identified. At this stage, we finished the *Stage 4* (papers selection) and the *Stage 5* (quality evaluation) of the SLR process (Fig. 1). The remaining articles were selected to be further analyzed and their data extracted for future evaluation and implementation of the last phase of the SLR (documenting).

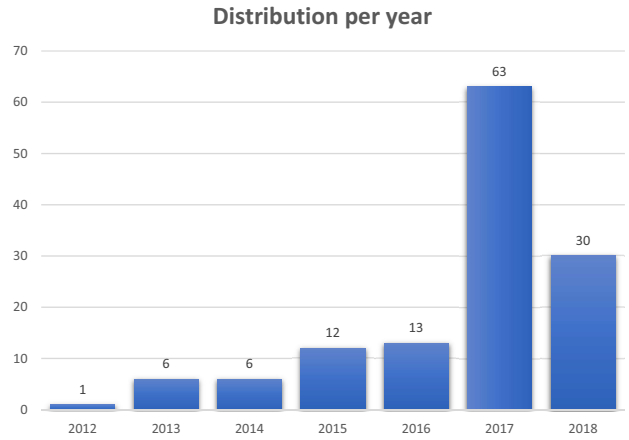


Fig. 3. Distribution of the primary studies per year.

B.2 Data Extraction and Synthesis

After the selection of the 131 primary studies, the *Stage 6* of the SLR consists of data extraction and progress monitoring. So, the data of these papers were included in a data extraction table for the subsequent steps. The attributes for the data extraction table are described below:

- Id, Paper, Year, Journal, Main Challenges, App Domain, Authentication (Technique, Tier), Access Control (Technique, Tier), Data Protection (Technique, Tier), Trust (Technique, Tier), Notes, Status, Quality Criteria (QC1, QC2, QC3, Sum).

The last stage of the conducting phase consists of synthesizing the extracted data from the primary studies to answer the research questions, that will be detailed in Sections III and IV.

C. Documenting

Finally, the last two stages to the SLR are the *Stage 8* - reports and recommendations and *Stage 9* - results presentation. Both steps consist of preparing the reports and the results in a paper (or report) format. In the next sections, we present the obtained results, the analysis, the discussion and conclusions.

III. STATISTICS FOR SELECTED STUDIES

After selecting and analyzing the primary studies, in this section, quantitative descriptions of frequencies were used to evaluate and synthesize the primary studies in terms of their publication year, application domain and the architectural tier of the deployment security technique.

A. Distribution over the Years

It is well-known that security and data privacy are major challenges in the context of IoT. The distribution of primary studies over the years (Fig. 3) corroborates that these challenges have been the subject of study and with strong growth in recent years. It is important to note that more than 70% of the primary studies have been published in the last two years (2017 and 2018). If we consider the fact that this extraction was carried out in May 2018, it is not risky to suggest that the year of 2018 might exceed 2017 in the number of related publications.

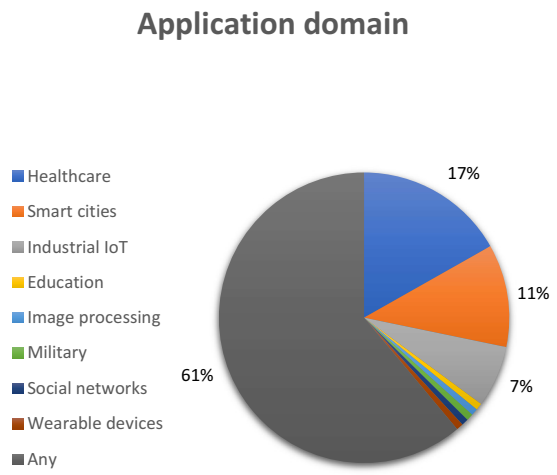


Fig. 4. General application domain.

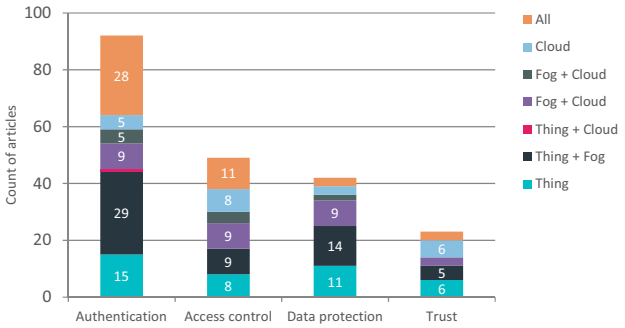


Fig. 5. Distribution of studies per tiers.

B. Application Domain

As shown in Fig. 4, the concern with security and data privacy issues is transversal because it embraces many application domains. Most of primary studies are focused on solutions that can be applied to any application domain (61%), followed by 17% studies that addressed healthcare and 11% of smart cities applications. The rest of publications are fairly distributed among specific domains, with a slight predominance for Industrial IoT (7%). These numbers indicate that our research object is a general concern in the context of IoT. Efficient approaches for handling security would have great potential to be adopted in a multitude of application domains and would represent a major advance in the field.

C. Deployment of Security Techniques at the Architectural Tiers

Considering the heterogeneity of IoT environments, computational resources of things vary from constrained devices that have limited CPU, memory, and power resources to more powerful ones. When the workload generated by an application is very demanding in terms of computational resources, it is common to move part of the computational effort from constrained IoT devices to other places with more resources. This process is known as computational offload and the natural candidate to accommodate the processing and long-term storage of the huge amount of IoT data is the cloud. By integrating IoT with the cloud, an ecosystem composed of two architectural tiers emerges, with the physical/things tier at the bottom and the cloud as the upper tier.

However, cloud-based IoT systems suffer from a number of limitations. The most prominent one is to deliver results in real time, as required by several IoT applications. Because clouds are clusters of data centers located in specific geographic locations, the network overhead of moving data into and outside the core of the cloud needs to be accounted for. Strict latency requirements are often incompatible with the unpredictable performance of cloud-based analytics or controllers [22]. Another drawback of using traditional cloud platforms for IoT applications is the nature of the data generated by many of these applications. As we discuss throughout this paper, sensors embedded in the environment often collect data of an extremely sensitive nature and send these data directly to remote data centers in the cloud without any kind of treatment or anonymization, which is not desirable, raising privacy and security concerns. In recent years, the frameworks of edge computing [23] or fog computing [24] have emerged as a solution for these above-mentioned issues. Instead of performing all the computations in the remote cloud, edge/fog computing proposes the decentralization of the computation through the offloading of some specific tasks to nodes at the edge of the network, which are closer to the data sources. Edge/fog nodes are devices not so computational powerful as cloud data centers, but are able to provide location-aware services and fast response to time-sensitive applications.

By adopting the edge computing approach, an intermediate tier of computing is introduced between the physical/IoT devices and the cloud, giving rise to a 3-tier IoT ecosystem. Therefore, the execution of both the workload generated by the applications and by infrastructure-level components, such as those responsible for the implementation of security aspects, can occur in one of these three tiers. The need arises to make decisions about the most appropriate tier to implement and deploy each security solution in an IoT System. Some security techniques require more extensive computing resources, while others need to be used as close to the data source as possible to ensure their privacy. Therefore, we consider that analyzing the retrieved studies from the prism of the architectural tier in which the presented techniques were implemented can help guiding the design decisions of developers.

We assume in this paper an architecture for IoT systems that comprises three distinct tiers: Thing, fog, and cloud, as proposed in [25]. The goal of considering where the techniques presented in the studies are implemented, in such architecture, is that the analysis carried out provide indications as to the tendencies with respect to such aspect.

However, as shown in Fig. 5, we did not observe a trend with regard to the placement of the proposed techniques, since there was a balanced distribution of solutions over all tiers. The only exception refers to the Authentication aspect, where the implementation in the “Thing + Fog” and “All” tiers had more articles. We believe that this behavior happens because authentication involves at least two entities, so for example, devices on Thing tier authenticate either with another device or with a member of superior tiers.

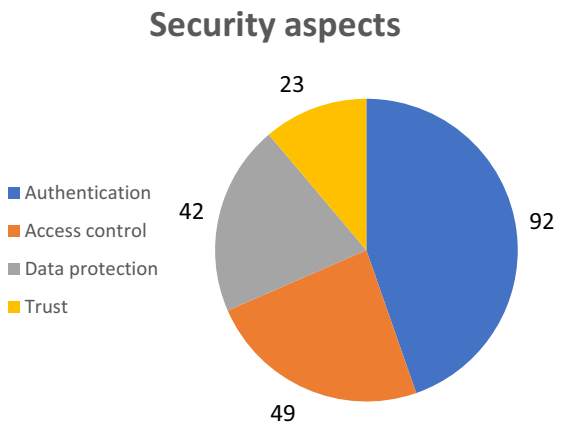


Fig. 6. Distribution of studies by security aspect.

IV. SECURITY ASPECTS ANALYSIS

In this section we discuss the data extracted from primary studies with the perspective of security aspects considered in this article to identify trends and research gaps.

A. General Aspects Analysis

Fig. 6 shows the number of studies that addressed each security aspect analyzed in this SLR. Most of papers covers techniques related to authentication, thus signaling a great interest of research in techniques that implement authentication in an IoT context. On the other hand, few studies have investigated trust issues, which is the aspect least addressed in the primary studies, although it is obviously of great relevance in the IoT context. With the tendency in IoT to adopt distributed transactions and more relaxed business models, without formal contracts, trust between the parties is fundamental. Thus, we consider the study and development of techniques that implement trust for the IoT context as a research gap that deserves further investigation.

Regarding access control and data protection, we verified a reasonable amount of studies that deal with these aspects, although not as significant as authentication. Still, in Fig. 6, we emphasize that absolute numbers were used instead of percentages since many papers addressed more than one security aspect. Thus, the number of articles that addressed each technique is higher than the number of selected primary studies.

B. Authentication

Authentication is the process of identifying a legitimate entity of a particular application [26]. As the authors in [27] state, device authentication has been shown to offer significant benefits to IoT security architecture and it became one of the most indispensable elements in IoT security ecosystems, due the fact that authentication is essential to offer other security aspects. Moreover, authentication acts as a first step of security for a system, which reduces its exposure to malicious software. Our performed literature review reinforces this assertion because, from the four aspects chosen for evaluation, this is the most frequently addressed on the primary studies, counting 92 related papers. Due to its high relevance, its distribution among the application domains does not differ significantly from the general view: Any (58 studies), healthcare (16 studies), smart cities (10 studies), Industrial IoT (4 studies), followed by education, image processing, military and wearable devices with 1 study each.

With this number, it is possible to affirm that authentication is an aspect widely studied and of great interest of the scientific community within IoT. There are some techniques that emerge as trends, with curious emphasis on two based on mechanisms originally designed to address other aspects of security: Elliptic-curve cryptography (ECC) and datagram transport layer security (DTLS), as can be seen in Table 4. While the former is essentially an encryption technique, the latter falls within the group of communication protocols.

The studies that implemented these techniques share the same challenge of dealing with resource-constrained devices. Lightweight approaches for these techniques were observed to fit the universe of wireless sensors networks and IoT. In [28] security keys using elliptic curve digital signature algorithm (ECDSA) with hash message digest are assigned to IoT nodes. A DTLS handshake step at the edge (gateway) [29] and a refined and lightweight version DTLS [27], [30] are good examples of these novel approaches. Besides these two, four other techniques originally designed for authentication also emerge as trends. These, in turn, can be classified into two groups by similarity: OAuth and OpenID, which are widely diffused as standards for web and distributed applications in general; and biometrics and physical unclonable function (PUF), techniques strongly related to physical devices.

It is important to remark that “Author Solution” stands for proprietary techniques that were proposed in the respective studies but not widely spread or adopted yet.

Contrary to the trends identified for the choice of techniques, the implementation tier of them does not present any clear preference in the selected studies. Although there is a slight predominance for "Thing + Fog" tiers, it is reasonable to say that Authentication solutions are distributed and can be present in all tiers of the reference architecture.

C. Access Control

Access control is the process of controlling requests to some resource from an authorized entity, allowing or denying access according to specified rules [69]. This aspect was unfolded as the second most found among primary studies counting 49 articles. Most of studies concentrates in no specific application, classified as “Any” (25 studies), followed by healthcare applications (12 studies), smart cities (6 studies), Industrial IoT (4 studies), and education and military (1 study each).

Due to the number of studies that cover access control, we might say that this is a quite relevant research area and reveals tendency regarding the adoption of some techniques. Table 5 shows the most relevant techniques, presenting blockchain (BC) as a promising one. The adoption of BC allows removing the need for a third-party institution that intermediate all transactions between entities (things). Considering that IoT takes advantage of opportunistic interactions (random or serendipity encounters), establishing trust between devices is challenging since the devices might not be known by each other and they can potentially be tampered. This way, BC approach could help to deal with this challenge, providing an infrastructure that devices could check the trustability of the devices. BC was originally

Table 4. Top techniques for authentication grouped by tiers.

Technique	Tier	Studies
Elliptic-curve cryptography (ECC)	Thing; Thing + Fog; Thing + Cloud; Fog; All	[26]–[28], [31]–[37]
Author solution	Thing + Fog; Fog; Cloud; All	[38]–[47]
OAuth	Thing + Fog; Fog; Fog + Cloud; Cloud; All	[48]–[53]
Datagram transport layer security (DTLS)	Fog; All	[29], [45], [54]–[59]
Biometric	Thing; Thing + Fog	[60]–[64]
OpenId	Thing + Fog; Fog + Cloud	[52], [53], [65]
Physical unclonable functions (PUF)	Thing + Fog; All	[66]–[68]

proposed for cryptocurrencies applications, but it rapidly spread to several other applications, serving as distributed database to store transactions in a tamper-proof manner. As an emerging technology, BC appears as a solution for access control in quite recent studies. For instance, in [70], the author presents an architecture based on BC to provide a fully distributed access control system and arbitrate roles and permissions for IoT applications. Ouaddah *et al.* [71] propose an access control framework called FairAccess which uses transactions on BC to grant, get, delegate and revoke access. Authors in [72] present four BC's, each one responsible for (i) interactions between things; (ii) context; (iii) accountability; and (iv) access rules, that intents to generalize different access control models. BC solutions do not focus on any specific application domain, and most of them are implemented in the fog or in cloud, not at the things. This makes sense because it is too expensive for a thing to contain the entire chain of transactions and to participate in the mining process.

Other techniques that stand out are attribute-based access control (ABAC) and the ones that we name "Author Solution" meaning proprietary solutions proposed by respective authors of analyzed studies. Regarding ABAC, this technique basically uses attributes from users, environment, among others, to create policies to control access. The authors in [76] propose an extension for message queue telemetry transport (MQTT) to provide a secure publish/subscribe system, not only considering authentication techniques, but also policy enforcement using ABAC. This technique is interesting for security since it provides access control based on information beyond user's authentication, that is, for example, the need to comply with specific attributes, like being in a given place, having a certain age, among others, that must be in accordance with applications requirements to allow some user operation. In general, attribute-based approaches are relevant for IoT since they provide more flexibility for applications by allowing direct addressing data instead of communication endpoints, which complies with data-centric systems (as IoT). Besides, these techniques provide context-aware characteristics, which makes access control challenging since more granular rules will be needed to control access to more available data. Then, the analyzed studies cover what makes access control a challenge, for instance, the mobility of nodes, the number of connected nodes and their vulnerabilities to be tampered, as well as their opportunistic interactions.

In terms of the implementation place, access control techniques were spread implemented, revealing implementations at the Things, Fog, and Cloud, tiers. It means that there is no trend about the most suitable place to deploy access control solutions. Nevertheless, most of studies involving healthcare, smart cities, and Industrial IoT applications tend to implement access control outside things. This approach unfolds an evident concern about having lightweight solutions to keep the devices alive for as long as possible, which make sense specially in these types of applications. Within each tier of implementation there is no tendency revealed for a specific technique, in the same way that within each application domain.

D. Data Protection

As presented in [88], data protection essentially concerns the accountability to enable individual control over personal data flow, making a commitment from the data collection step through the data dissemination, data processing, and data storage, i.e., a total fine-grained data management. Most of the techniques found in the primary studies are based on encryption to provide data protection. This might be justified by the fact that the ECC technique and others are used. For example, according to [89], the elliptical curve digital signature algorithm (ECDSA) technique uses ECC to create a digital signature of data in order to allow verifying its authenticity without compromising overall performance. The size of the key used in ECDSA is only 160 bits, which is very small as compared to pure DSA. This reduces the communication overhead and improves the privacy of communication. The article also points out that ECDSA retains the privacy of communication and improves security against attackers, adding less number of bits to the original message as compared to common used encryption schemes (e.g. Rivest-Shamir-Adleman – RSA). This reduces the packet size and decreases the communication overhead, which contributes to a better performance of the security technique.

The authors in [90] point out specifically that public key cryptography (PKC) is considered unfeasible for wireless sensor networks in the early stages, so symmetric key-based security architectures were designed for this field. In [91], the authors mention that with the rapid development of Industrial IoT (IIoT), a large number of resource-constrained devices with limited communication, energy, and bandwidth is being used, which requires the search for lightweight security methods, which certainly makes data protection a research challenge. The authors implement an authentication and key agreement mechanism based on implicit certificate, that is proposed based on open platform communications unified architecture (OPC UA) security model. In the process of establishing a secure channel, the lightweight ECC encryption algorithm is adopted to ensure the security of data transmission in the communication process. So, the authors show that this mechanism could be used in resource-constrained environments. According to [52], ECC, unlike other

Table 5. Top techniques for access control grouped by tiers.

Technique	Tier	Studies
Blockchain	Fog; Cloud; ALL	[70]–[74]
Attribute-based access control (ABAC)	Thing+ Fog; Fog + Cloud; Cloud	[49], [75]–[77]
Author solutions	Fog; Cloud	[42], [45], [71]
Biometric	Thing; ALL	[78]–[80]
Smart card	Thing; Thing + Fog	[81]–[83]
Registration/subscription	Thing + Fog; ALL	[75], [84]
DCapBAC	Thing + Fog; Fog + Cloud	[52], [65]
Smart contracts	Fog	[70], [74]
Rule-based access control (RBAC)	FOG; Cloud	[49], [85]
SecIIot	Thing + Fog; Fog	[86], [87]

cryptographic schemes, requires lower computing and memory resources as well as smaller keys. With these studies we can see that it is possible to have data protection even on end devices, which is our suggestion if they are the origin of the data.

The implementation tier with more occurrences of data protection solutions was Thing + Fog. In general, this occurred due to the use of cryptographic techniques between these tiers, considering that data should be protected from its origin, as commented before. In this way, appropriated techniques to the computational constraints in each tier of the proposed architecture should be used, which consider restricted devices and a resource-rich edge, approximating data protection implementation to the place from where data is generated.

In Table 6, the most relevant techniques found in the primary studies cover cryptographic solutions, with prominence to ECC-based approaches. This behavior suggests a direct relation between data protection and authentication techniques. The three application domains with more occurrences, excluding the general domain (Any), were healthcare, smart cities and Industrial IoT. This observation reveals a correspondence to other aspects and to the general case. Also, we can observe that ECC and AES are commonplace techniques for this security aspect.

E. Trust

The concept of trust is different for human community and IoT devices. Among people, trust is built based not only on others' behavior and reputation, but also on the experience, knowledge, and other attributes of the observer. For instance, the trust level assigned by an observer to another person can be influenced by cultural and environmental aspects of the observer. On the other hand, for IoT devices A and B, the trust level assigned to B by A is based only on the behavior of B, i.e., the behavior of A does not influence the evaluation of trust of B.

According to [102], trust is a complicated concept, which comprises many aspects such as confidence, belief, integrity, among others. Considering this fact along with our analysis, we come to a concept of trust that comprises identity assurance, device's behavior, data integrity and protection. Therefore, trust spreads through other aspects considered in this study such as authentication and data protection.

Out of the 131 primary studies selected, only 23 papers addressed techniques related to trust, so this was the aspect least addressed by the studies. It's important to note that some studies discussed more than one security aspect, such as [84] that covered trust, data protection and access control techniques.

Regarding the place of the trust techniques implementation in terms of the architectural tiers considered in this study, we verified the existence of a balanced distribution, since 6 studies implemented their technique in the Cloud, 6 in the Thing tier, 5 Thing + Fog, 3 in all tiers and 3 implemented in the Fog. Considering this even distribution of the implementation of these techniques among the tiers, it was not possible to verify any trend of trust techniques regarding the placement of their code. Likewise, as presented in [102], considering subjective user properties related to the concept of trust, it becomes difficult to identify where trust techniques should be implemented, making the choice of location of the implementation dependent on the application features. For instance, in [103] authors choose to implement the trust solution in Cloud since the application requirement for classifying nodes has heavy computational effort to be placed on another tier. Nguyen *et al.* [104] present a lightweight trust solution implemented on things to deliver an initial trust level for devices that have not previously encountered each other within the range of a personal area network (PAN). So, the solution was implemented at the Thing tier.

With respect to the techniques themselves, no highlights could be observed. Of the 23 papers, two used blockchain-based solutions, while the other papers applied different techniques, as shown in Table 7, which depicts the techniques used by the 10 best articles according to the quality criteria stipulated for this secondary study. It is worth mentioning that these quality criteria do not relate to the best articles in general, but to those that best fit the criteria that this study aimed to verify.

A relevant fact related to the techniques employed was the use of blockchain to guarantee trust. Because it is an emerging technology, blockchain still presents some shortcomings, among them issues related to scalability [109]. In [109], authors propose a food supply chain traceability system for real-time food tracking based on the implementation of blockchain. As described in Section IV.C, authors in [71] proposed FairAccess, a framework for access control in IoT based on Blockchain, that, besides giving access control solution, gives trust solution also.

Finally, based on the lack of standardization of techniques to implement trust and the small number of studies that have presented proposals for this aspect, we consider trust a research gap. A more detailed study of such aspect would be important and necessary, with a particular focus on standardization and convergence of definitions and techniques.

Table 6. Top techniques for data protection grouped by tiers.

Technique	Tier	Studies
Elliptic-curve cryptography (ECC)	Thing; Thing + Fog; Cloud; All	[27], [37], [52], [83], [90]–[94]
Advanced encryption standard (AES)	Thing + Fog; Cloud	[45], [93], [95], [96]
Cryptography	Fog; Thing + Fog; All	[48], [60], [84], [97]
Attribute-based encryption (ABE)	Thing + Fog; Fog + Cloud	[98], [99]
Datagram transport layer security (DTLS)	Thing + Fog	[99], [100]
Elliptic-curve digital signature algorithm (ECDSA)	Fog; Thing + Fog	[71], [89]
OpenSSL	Thing + Fog	[42], [45]
XOR operations	Thing; Fog	[78], [79]
Blockchain	Fog	[73]
One time password (OTP)	Fog + Cloud	[101]

Table 7. Top techniques for trust grouped by tiers.

Technique	Tier	Studies
Couterfeit detection, traceability and authentication (CDTA)	Thing	[92]
Author solution	Thing	[28], [104]
MRC scheme with TM security algorithm	Thing	[105]
Knowledge base systems (KBS)	Cloud	[93]
Social-based trusted solution	Cloud	[106]
Malleable signature schemes (MSS)	Thing	[107]
Fuzzy	Thing + Fog	[52]
Remote attestation model	Thing + Fog	[108]
Machine learning	Cloud	[103]
Elastic slide window	Cloud	[103]

V. DISCUSSION

Through the analysis of the obtained results, we could identify that trust in IoT is a research gap with few studies exploring this aspect. Also, a considerable number of studies that dealt with authentication aspect, using ECC, "Author Solutions" and OAuth-based techniques. The ECC technique is reasonable to appear in this aspect since it is well-established. The "Author Solutions" is a mix of different solutions proposed by the authors of the primary studies. And what catches some attention is the adoption of OAuth-based techniques that was thought to be an open standard for API access delegation.

Concerning the decision regarding the deployment of security solutions (in a 3-tier IoT architecture), our analysis showed that, for authentication, a minimum of two entities are involved in the authentication process. The entities might belong to a specific tier or to more than one tier. This way, the place of authentication implementation should be the same of those entities' tier. For access control, the deployment of solutions regarding this security aspect should consider lightweight implementations at the Thing tier whenever possible and pervade all other tiers in which an IoT application resides. Concerning data protection, the implementation of this aspect should be done from the data generation to all involved tiers, traversing the entire life cycle of data processing. Similar to access control, the implementation of trust techniques should consider all tiers covered by an IoT application. These results underscore the holistic nature of security solutions for IoT. In order to achieve the true potential of this technology, it is essential to develop systems where security permeates all tiers from the moment a sensitive data gains some context to its consumption by the user's applications.

Almost all analyzed studies were published in the last three years, which shows an increasing interest on IoT security by the research community. This also indicates that more attention might be expected to this area on the upcoming years. Among eliminated studies, a significant number of those that lack from experiments that would evaluate their approaches and solutions, which helps readers to confirm their feasibility and efficiency.

We would like to highlight the importance of having a holistic view of security to protect IoT building blocks and provide security by design. Finally, there is a lack of a well-defined architecture that considers security aspects that could serve as a reference architecture to develop IoT security solutions.

VI. CONCLUDING REMARKS

In order to obtain the studies to be analyzed in this paper, we followed a meticulous and systematic process. We presented our research methodology through an SLR and showed the details of the searches and the obtained results, besides providing some numerical data. As future studies, we aim to consider other security aspects (e.g., privacy and secure middleware), so as to present different perspectives of security in IoT. We also intend to follow the results of our study to pursue the revealed trends and propose new techniques to overcome research gaps.

REFERENCES

[1] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, Oct 2010.
[2] Ericsson, "Ericsson mobility report," Tech. Rep., Ericsson, 2017.
[3] A. Al-Fuqaha *et al*, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347–2376, Fourthquarter 2015.
[4] K. T. Nguyen, M. Laurent, and N. Oualha, "Survey on secure commu-

nication protocols for the internet of things," *Ad Hoc Netw.*, vol. 32, pp. 17–31, 2015.
[5] K. Zhao and L. Ge, "A survey on the internet of things security," in *Proc. CISIS*, Dec. 2013, pp. 663–667.
[6] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the internet of things: Perspectives and challenges," *Wireless Netw.*, vol. 20, pp. 2481–2501, Nov. 2014.
[7] S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: The road ahead," *Comput. Netw.*, vol. 76, pp. 146–164, Jan. 2015.
[8] I. Ali and Z. Ullah, "Internet of things security, device authentication and access control: A review," *International J. Comput. Science Inf. security*, vol. 14, no. 8, Aug. 2016, pp. 456–466.
[9] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of things security: A survey," *J. Netw. Comput. Appl.*, vol. 88, pp. 10–28, June 2017.
[10] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of things security: A top-down survey," *Comput. Netw.*, vol. 141, pp. 199–221, Aug. 2018.
[11] M. Ammar, G. Russello, and B. Crispo, "Internet of things: A survey on the security of IoT frameworks," *J. Inf. Security Appl.*, vol. 38, pp. 8–27, Feb. 2018.
[12] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Generation Comput. Syst.*, vol. 82, pp. 395–411, May 2018.
[13] A. R. Sfar, E. Natalizio, Y. Challal, and Z. Chtourou, "A roadmap for security challenges in the internet of things," *Digital Commun. Netw.*, vol. 4, no. 2, pp. 118–137, Apr. 2018.
[14] M. Irshad, "A Systematic Review of Information Security Frameworks in the internet of things," in *Proc. IEEE HPCC*, Dec. 2016, pp. 1270–1275.
[15] B. Kitchenham *et al*, "Systematic literature reviews in software engineering – a systematic literature review," *Inf. Software Tech.*, vol. 51, no. 1, pp. 7–15, Jan. 2009.
[16] P. Brereton, B. A. Kitchenham, D. Budgen, M. Turner, and M. Khalil, "Lessons from applying the systematic literature review process within the software engineering domain," *J. Syst. Software*, vol. 80, no. 4, pp. 571–583, Apr. 2007. Software Performance.
[17] E. Cavalcante *et al*, "On the interplay of internet of things and cloud computing: A systematic mapping study," *Comput. Commun.*, vol. 89-90, pp. 17 – 33, Sept. 2016.
[18] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in internet-of-things," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1250–1258, Oct. 2017.
[19] B. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering," Tech. Rep. EBSE2007-01, 2007.
[20] C. M. D. Farias *et al*, "A systematic review of shared sensor networks," *ACM Comput. Surv.*, vol. 48, no. 4, pp. 1–50, Feb. 2016.
[21] C. Wohlin *et al*, *Experimentation in Software Engineering: An Introduction*. Norwell, MA, USA: Kluwer Academic Publishers, 2000.
[22] B. Zhang *et al*, "The cloud is not enough: Saving iot from the cloud," in *Proc. USENIX Workshop*, July 2015.
[23] P. Garcia Lopez *et al*, "Edge-centric computing: Vision and challenges,"*SIGCOMM Comput. Commun. Rev.*, vol. 45, no. 5, pp. 37–42, Sept. 2015. 2015.
[24] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," in *Proc. ACM MCC Workshop*, Aug. 2012, pp. 13–16.
[25] W. Li *et al*, "System modelling and performance evaluation of a three-tier cloud of things," *Future Generation Comput. Syst.*, vol. 70, pp. 104–125, May 2017.
[26] S. Kalra and S. K. Sood, "Secure authentication scheme for IoT and cloud servers," *Pervasive and Mobile Comput.*, vol. 24, pp. 210–223, Dec. 2015.
[27] K. H. Yeh, "A Secure IoT-based healthcare system with body sensor networks," *IEEE Access*, vol. 4, pp. 10288–10299, Dec. 2016.
[28] M. B. Krishna and P. Lorenz, "Delay aware secure hashing for opportunistic message forwarding in internet of things," in *Proc. IEEE GLOBECOM Workshops*, Dec. 2017, pp. 1–6.
[29] A. Rajagopalan, M. Jagga, A. Kumari, and S. T. Ali, "A DDoS prevention scheme for session resumption SEA architecture in healthcare IoT," in *Proc. IEEE CICT*, Feb. 2017, pp. 1–5.
[30] S. L. Keoh, S. S. Kumar, and H. Tschofenig, "Securing the internet of things: A standardization perspective," *IEEE Internet Things J.*, vol. 1, no. 3, June 2014.
[31] S. C. Cha, J. F. Chen, C. Su, and K. H. Yeh, "A blockchain connected gateway for BLE-based devices in the internet of things," *IEEE Access*, vol. 6, pp. 24639–24649, Jan. 2018.
[32] J. Shen, S. Chang, J. Shen, Q. Liu, and X. Sun, "A lightweight multilayer authentication protocol for wireless body area networks," *Future Generation Comput. Syst.*, vol. 78, pp. 956–963, Jan. 2018.
[33] M. Turkanović, B. Brumen, and M. Hölbl, "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the internet of things notion," *Ad Hoc Netw.*, vol. 20, pp. 96–112, Sept. 2014.
[34] K.-H. Wang, C.-M. Chen, W. Fang, and T.-Y. Wu, "A secure authentication scheme for internet of things," *Pervasive and Mobile Comput.*, vol. 42, pp. 15–26, Dec. 2017.
[35] X. Zhang, S. Poslad, and Z. Ma, "A semi-outsourcing secure data privacy scheme for IoT data transmission," in *Proc. IEEE PIMRC*, Oct. 2017, pp. 1–5.
[36] Z. Mahmood *et al*, "Secure authentication and prescription safety protocol for telecare health services using ubiquitous IoT," *Applied Sciences*, vol. 7, p. 1069, Oct. 2017.
[37] S. Ullah, B. Rinner, and L. Marcenaro, "Smart cameras with onboard signcryption for securing IoT applications," in *Proc. IEEE GIoTS*, June 2017, pp. 1–6.
[38] R. Amin, N. Kumar, G. Biswas, R. Iqbal, and V. Chang, "A light weight authentication protocol for IoT-enabled devices in distributed cloud computing environment," *Future Generation Comput. Syst.*, vol. 78, pp. 1005–1019, Jan. 2018.
[39] F. Wu *et al*, "A lightweight and privacy-preserving mutual authentication scheme for wearable devices assisted by cloud server," *Comput. Electrical Engineering*, vol. 63, pp. 168–181, Oct. 2017.
[40] F. Wu *et al*, "A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks," *Future Generation Comput. Syst.*, vol. 82, pp. 727–737, May 2018.
[41] Z. Wang, "A privacy-preserving and accountable authentication protocol for IoT end-devices with weaker identity," *Future Generation Comput. Syst.*, vol. 82, pp. 342–348, May 2018.
[42] M. Tao, K. Ota, M. Dong, and Z. Qian, "AccessAuth: Capacity-aware security access authentication in federated-IoT-enabled V2G networks," *J. Parallel Distributed Comput.*, vol. 118, no. 1, pp. 107–117, Aug. 2018.
[43] M. S. Farash, M. Turkanović, S. Kumari, and M. Hölbl, "An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the internet of things environment," *Ad Hoc Netw.*, vol. 36, no. 1, pp. 152–176, Jan. 2016.
[44] W.-L. Tai, Y.-F. Chang, and W.-H. Li, "An IoT notion–based authentication and key agreement scheme ensuring user anonymity for heterogeneous ad hoc wireless sensor networks," *J. Inf. Security Appl.*, vol. 34, no. 2, pp. 133–141, June 2017.
[45] S. R. Moosavi *et al*, "End-to-end security scheme for mobility enabled healthcare internet of things," *Future Generation Comput. Syst.*, vol. 64, pp. 108–124, Nov. 2016.
[46] X.-J. Lin, L. Sun, and H. Qu, "Insecurity of an anonymous authentication for privacy-preserving IoT target-driven applications," *Comput. Security*, vol. 48, pp. 142–149, Feb. 2015.
[47] Y.-Y. Deng, C.-L. Chen, W.-J. Tsaur, Y.-W. Tang, and J.-H. Chen, "Internet of things (IoT) based design of a secure and lightweight body area network (BAN) Healthcare System," *Sensors*, vol. 17, no. 12, p. 2919, Dec. 2017.
[48] L. A. B. Pacheco, E. Alchieri, and P. A. Barreto, "Enhancing and evaluating an architecture for privacy in the integration of internet of things and cloud computing," in *Proc. IEEE NCA*, Jan. 2017, pp. 1–8.
[49] A. Álonso, F. Fernández, L. Marco, and J. Salvachúa, "IAACaaS: IoT application-scoped access control as a service," *Future Internet*, vol. 9, no. 4, pp. 1–14, July 2017.
[50] S. Kinikar and S. Terdal, "Implementation of open authentication protocol for IoT based application," in *Proc. IEEE ICICT*, Aug. 2016, pp. 1–4.
[51] S. Cirani, M. Picone, P. Gonizzi, L. Veltri, and G. Ferrari, "IoT-OAS: An OAuth-based authorization service architecture for secure services in IoT scenarios," *IEEE Sensors J.*, vol. 15, pp. 1224–1234, Feb. 2015.
[52] J. Bernal Bernabe, J. L. Hernandez Ramos, and A. F. Skarmeta Gomez, "TACIoT: multidimensional trust-aware access control system for the internet of things," *Soft Comput.*, vol. 20, no. 5, pp. 1763–1779, May 2016.
[53] S. H. Lee, K. W. Huang, and C. S. Yang, "TBAS: Token-based authorization service architecture in internet of things scenarios," *International J. Distributed Sensor Netw.*, vol. 13, no. 7, July 2017.
[54] T. Kothmayr, C. Schmitt, W. Hu, M. Brunig, and G. Carle, "A DTLS based end-to-end security architecture for the internet of things with two-way authentication," in *Proc. IEEE LCN Workshops*, Oct. 2012, pp. 956–963.
[55] G. Lessa dos Santos, V. T. Guimaraes, G. da Cunha Rodrigues, L. Z. Granville, and L. M. R. Tarouco, "A DTLS-based security architecture for the internet of things," in *Proc. IEEE ISCC*, July 2015, pp. 809–815.

[56] M. A. ElAffendi and A. L. Alamudy, "Could virtualization be the ultimate solution for IoT resource constrained devices problem? A multilevel security framework based on device virtualization," in *Proc. ICCA*, Sept. 2017, pp. 232–237.

[57] R. Hummen, H. Shafagh, S. Raza, T. Voig, and K. Wehrle, "Delegation-based authentication and authorization for the IP-based internet of things," in *Proc. SECON*, June 2014, pp. 284–292.

[58] T. Kothmayr, C. Schmitt, W. Hu, M. Brünig, and G. Carle, "DTLS based security and two-way authentication for the internet of things," *Ad Hoc Netw.*, vol. 11, pp. 2710–2723, Nov. 2013.

[59] S. R. Moosavi *et al.*, "SEA: A secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways," *Procedia Comput. Science*, vol. 52, pp. 452–459, Jan. 2015.

[60] X. Li *et al*, "A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments," *J. Netw. Comput. Appl.*, vol. 103, no. 1, pp. 194–204, Feb. 2017.

[61] P. Peris-Lopez, L. González-Manzano, C. Camara, and J. M. de Fuentes, "Effect of attacker characterization in ECG-based continuous authentication mechanisms for internet of things," *Future Generation Comput. Syst.*, vol. 81, pp. 67–77, Apr. 2018.

[62] Y. Lu *et al*, "Exploring finger vein based personal authentication for secure IoT," *Future Generation Comput. Syst.*, vol. 77, pp. 149–160, Dec. 2017.

[63] J. Srinivas, S. Mukhopadhyay, and D. Mishra, "Secure and efficient user authentication scheme for multi-gateway wireless sensor networks," *Ad Hoc Netw.*, vol. 54, pp. 147–169, Jan. 2017.

[64] M. W. Condry and C. B. Nelson, "Using smart edge IoT devices for safer, rapid response with industry IoT control operations," *Proc. IEEE*, vol. 104, no. 5, May 2016, pp. 938–946.

[65] M. Hossain, S. M. Islam, F. Ali, K. S. Kwak, and R. Hasan, "An internet of things-based health prescription assistant and its security system design," *Future Generation Comput. Syst.*, vol. 82, pp. 422–439, May 2018.

[66] U. Chatterjee, R. S. Chakraborty, and D. Mukhopadhyay, "A PUF-based secure communication pProtocol for IoT," *ACM Trans. Embedded Comput. Syst.*, vol. 16, no. 3, pp. 1–25, Apr. 2017.

[67] W. Feng, Y. Qin, S. Zhao, and D. Feng, "AAoT: Lightweight attestation and authentication of low-resource things in IoT and CPS," *Comput. Netw.*, vol. 134, pp. 167–182, Apr. 2018.

[68] C. Huth, J. Zibuschka, P. Duplys, and T. Guneysu, "Securing systems on the internet of things via physical properties of devices and communications," in *Proc. IEEE SysCon*, Apr. 2015, pp. 8–13.

[69] R. Sandhu and P. Samarati, "Access control: Principle and practice," *IEEE Commun. Mag.*, vol. 32, no. 9, pp. 40–48, Sept. 1994.

[70] O. Novo, "Blockchain Meets IoT: An architecture for scalable access management in IoT," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1184–1195, Mar. 2018.

[71] A. Ouaddah, A. Abou Elkalam, and A. Ait Ouahman, "FairAccess: A new blockchain-based access control framework for the internet of things," *Security and Commun. Netw.*, vol. 9, no. 18, pp. 5943–5964, Dec. 2016.

[72] O. J. A. Pinno, A. R. A. Gregio, and L. C. De Bona, "ControlChain: Blockchain as a central enabler for access control authorizations in the IoT," in *Proc. IEEE GLOBECOM*, Dec. 2018, pp. 1–6.

[73] N. Baracaldo *et al*, "Securing data provenance in internet of things (IoT) systems," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 10380, pp. 92–98, Oct. 2017.

[74] N. Rifi, E. Rachkidi, N. Agoulmine, and N. C. Taher, "Towards using blockchain technology for eHealth data access management," in *Proc. IEEE ICABME*, Oct. 2017, pp. 1–4.

[75] A. Alshehri and R. Sandhu, "Access control models for virtual object communication in cloud-enabled IoT," in *Proc. IEEE IRI*, Jan. 2017, pp. 16–25.

[76] A. Rizzardi, S. Sicari, D. Miorandi, and A. Coen-porisini, "AUPS : An open source authenticated publish / subscribe system for the internet of things," *Inf. Syst.*, vol. 62, pp. 29–41, Dec. 2016.

[77] U. Salama, L. Yao, X. Wang, H. Y. Paik, and A. Beheshti, "Multi-level privacy-preserving access control as a service for personal healthcare monitoring," in *Proc. IEEE ICWS*, June 2017, pp. 878–881.

[78] N. Kadham and K. Sreenivasa Ravi, "A lightweight one time password (OTP) based smart learning in internet of things," *International J. Engineering Tech.*, vol. 7, no. 2.7, pp. 480–483, Mar. 2018.

[79] P. K. Dhillon and S. Kalra, "A lightweight biometrics based remote user authentication scheme for IoT services," *J. Inf. Security Appl.*, vol. 34, no. 2, pp. 255–270, June 2017.

[80] D. Shah and V. Haradi, "IoT based biometrics implementation on raspberry Pi," *Procedia Comput. Science*, vol. 79, pp. 328–336, Dec. 2016.

[81] F. Wu *et al*, "An efficient authentication and key agreement scheme for multi-gateway wireless sensor networks in IoT deployment," *J. Netw. Comput. Appl.*, vol. 89, pp. 72–85, July 2017.

[82] F. Wu, L. Xu, S. Kumari, and X. Li, "A privacy-preserving and provable user authentication scheme for wireless sensor networks based on internet of things security," *J. Ambient Intelligence Humanized Comput.*, vol. 8, no. 1, pp. 101–116, Feb. 2017.

[83] T. D. P. Bai and S. A. Rabara, "Design and development of integrated, secured and intelligent architecture for internet of things and cloud computing," in *Proc. IEEE FiCloud*, Aug. 2015, pp. 817–822.

[84] M. Taylor, D. Reilly, and B. Lempereur, "An access control management protocol for internet of things devices," *Netw. Security*, vol. 2017, no. 7, pp. 11–17, July 2017.

[85] X. Huang, P. Craig, H. Lin, and Z. Yan, "SecIoT: A security framework for the internet of things," *Security and Commun. Netw.*, vol. 9, pp. 3083–3094, Nov. 2016.

[86] G. Chen and W. S. Ng, "An efficient authorization framework for securing industrial internet of things," in *Proc. IEEE TENCON*, Nov. 2017, pp. 1219–1224.

[87] G. Chen and W. S. Ng, "An efficient authorization framework for securing industrial internet of things," in *Proc. IEEE TENCON*, Dec. 2017, pp. 1219–1224.

[88] A. Crabtree, T. Lodge, J. Colley, C. Greenghalgh, and R. Mortier, "Accountable internet of things? Outline of the IoT databox model," in *Proc. IEEE WoWMoM*, June 2017, pp. 1–6.

[89] M. B. Tamboli and D. Dambawade, "Secure and efficient CoAP based authentication and access control for internet of things (IoT)," in *Proc. IEEE RTEICT*, May 2016, pp. 1245–1250.

[90] M. Lavanya and V. Natarajan, "Lightweight key agreement protocol for IoT based on IKEv2," *Comput. Electrical Engineering*, vol. 64, pp. 580–594, Nov. 2017.

[91] M. Wei, S. Zhang, P. Wang, and K. Kim, "An authentication and key agreement mechanism for OPC unified architecture in industrial internet of things," *International J. Distributed Sensor Netw.*, vol. 14, pp. 1–11, Jan. 2018.

[92] K. Yang, D. Forte, and M. M. Tehranipoor, "Cdta: A comprehensive solution for counterfeit detection, traceability, and authentication in the iot supply chain," *ACM Trans. Des. Autom. Electron. Syst.*, vol. 22, no. 3, pp. 1–31, Apr. 2017.

[93] a. J. Jara, M. a. Zamora-Izquierdo, and a. F. Skarmeta, "Interconnection framework for mHealth and remote monitoring based on the internet of things," *IEEE J. Selected Areas Commun.*, vol. 31, no. 9, pp. 47–65, Aug. 2013.

[94] M. Saadeh, A. Sleit, K. E. Sabri, and W. Almobaideen, "Lightweight identity based signature for mobile object authentication in the internet of things," *J. Theoretical and Applied Inf. Technol.*, vol. 96, no. 3, pp. 788–798, Feb. 2018.

[95] M. A. Jan, F. Khan, M. Alam, and M. Usman, "A payload-based mutual authentication scheme for internet of things," *Future Generation Comput. Syst.*, vol. 92, pp. 1028–1039, Mar. 2019.

[96] P. Hu *et al*, "Security and privacy preservation scheme of face identification and resolution framework using fog computing in internet of things," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1143–1155, Oct. 2017.

[97] B. Ndibanje *et al*, "A Secure and efficient mutual authentication handoff protocol for sensors devices support in internet of things," *Sensors Materials*, vol. 29, no. 7, p. 1, Jan. 2017.

[98] S. Zebboudj *et al*, "Big data source location privacy and access control in the framework of IoT," in *Proc. ICEE-B*, Oct. 2017, pp. 1–5.

[99] J. Choi, Y. In, C. Park, S. Seok, H. Seo, and H. Kim, "Secure IoT framework and 2D architecture for end-To-end security," *J. Supercomputing*, vol. 74, no. 8, pp. 3521–3535, Aug. 2018.

[100] A. Haroon, S. Akram, M. A. Shah, and A. Wahid, "E-Lithe: A lightweight secure DTLS for IoT," in *Proc. IEEE VTC*, Sept. 2017, pp. 1–5.

[101] S. Lee *et al*, "Design and implementation for data protection of energy iot utilizing otp in the wireless mesh network," *Energy Procedia*, vol. 141, pp. 540–544, Dec. 2017.

[102] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for internet of things," *J. Netw. Comput. Appl.*, vol. 42, pp. 120–134, June 2014.

[103] J. Caminha, A. Perkusich, and M. Perkusich, "A smart trust management method to detect on-off attacks in the internet of things," *Security Commun. Netw.*, vol. 2018, pp. 1–10, Apr. 2018.

[104] T. Nguyen, D. Hoang, D. Nguyen, and A. Seneviratne, "Initial trust establishment for personal space iot systems," in *Proc. IEEE INFOCOM Workshop*, May 2017, pp. 784–789.

[105] J. I. Chen and D. J. Chuang, "Embedding of mrc in tm to increase the

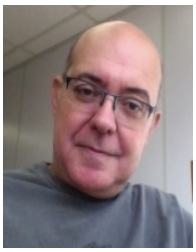
security for iot technologies," in *Proc. IEEE iCAST*, Nov. 2017, pp. 199–204.
[106] L. Militano, A. Orsino, G. Araniti, and A. Iera, "NB-IoT for D2D-enhanced content uploading with social trustworthiness in 5g systems," *Future Internet*, vol. 9, no. 3, July2017.
[107] H. C. Pöhls *et al*, "Rerum: Building a reliable iot upon privacy- and security- enabled smart objects," in *Proc. IEEE WCNCW Workshop*, Apr. 2014, pp. 122–127.
[108] B. Gong, Y. Zhang, and Y. Wang, "A remote attestation mechanism for the sensing layer nodes of the internet of things," *Future Generation Comput. Syst.*, vol. 78, pp. 867–886, Jan. 2018.
[109] F. Tian, "A supply chain traceability system for food safety based on haccp, blockchain amp;amp; internet of things," in *Proc. ICSSSM*, June 2017, pp. 1–6.

Evandro L. C. Macedo received his B.S. degree on Computing and Information Technology from State University of Rio de Janeiro (UERJ), Brazil in 2011. He acquired his Master's degree on Systems Engineering and Computing from the Systems Engineering and Computing Program , Federal University of Rio de Janeiro (UFRJ), Brazil in 2015. He is currently a Ph.D. student in Systems Engineering and Computing Program, UFRJ.

Egberto A. R. de Oliveira received his B.S. degree on Computing and Information Technology from State University of Rio de Janeiro (UERJ), Brazil in 2009. He is currently a M. SC. student in Systems Engineering and Computing Program at Federal University of Rio de Janeiro (PESC/COPPE/UFRJ) and Senior IT Analyst at Fundação Vale do Rio Doce de Seguridade Social (Valia). He is also a Microsoft Certified Solutions Expert: Cloud platform & infrastructure and AWS certified solutions architect - associate.

Fabio H. Silva received his Master degree in Computing and Systems from Military Institute of Engineering - IME (2010), graduate in Technology for Internet Systems from Federal Center for Technological Education of Rio de Janeiro - CEFET/RJ (2007). Currently is a Ph.D. student in Systems Engineering and Computing Program at Federal University of Rio de Janeiro - COPPE/UFRJ, technician in National Institute of Technology - INT, Assistant Professor in Carioca University Centre - Unicarioca.

Rui R. Mello Jr. received his B.Sc. degree in 2004 in Computer Science from Catholic University of Petrópolis. He received a M. Sc. degree in Systems Engineering and Computation from Federal University of Rio de Janeiro, in 2015. He is Lieutenant Commander from Brazilian Navy and member of the Brazilian Navy Research Institute. He is currently a D.Sc. student in Architectures and Operating Systems, System Engineering and Computation Program at Federal University of Rio de Janeiro.



Felipe M. G. França received his B.Sc. and M.Sc. degrees in Electronic Engineering and System Engineering and Computation, respectively, from Federal University of Rio de Janeiro (UFRJ), in 1982 and 1987. He received Ph.D. degree in Neural Systems Engineering from Imperial College of Science Technology and Medicine, in 1994. He is member of the Institute of Electrical and Electronics Engineers (IEEE) and Professor at UFRJ.

Flavia C. Delicato has a Ph.D. in Electrical and Computer Engineering (2005) from the Federal University of Rio de Janeiro. She is an Associate Professor of Computer Science at Federal University of Rio de Janeiro, Brazil. She is the author of 2 Books, more than 100 papers and participates in several research projects with funding from International and Brazilian government agencies. She is a level 1 Researcher Fellow of the Brazilian National Council for Scientific and Technological Development.

José F. de Rezende received B.Sc. and M.Sc. degrees in Electronics Engineering from Federal University of Rio de Janeiro in 1988 and 1991, respectively. He received the Ph.D. degree in Computer Science from Universit'e Pierre et Marie Curie in 1997. Since 1998 he has been an associate professor at UFRJ. He has served in the editorial board of Ad Hoc Networks from Elsevier since 2006.

Luís F. M. de Moraes received a B.S. and M.S. degrees in Electrical Engineering and Telecommunications from Pontifical Catholic University of Rio de Janeiro (PUC-Rio), in 1973 and 1976, respectively. He received Ph.D. degree in Electrical Engineering and System Science from University of California at Los Angeles (UCLA) in 1981. He is Professor at Federal University of Rio de Janeiro and technical-scientific coordinator of the REDERIO backbone, a pioneering Internet project in Rio de Janeiro, Brazil, supported by FAPERJ, since 1992.