Computer Science and Information Systems 12(1):161–184 DOI: 10.2298/CSIS140205086C

Security in Cloud Computing: a Mapping Study

Belén Cruz Zapata[1], José Luis Fernández-Alemán[1], and Ambrosio Toval[1]

[1] Faculty of Computer Science, Campus de Espinardo, 30100,
University of Murcia, Spain
{b.cruzzapata, aleman, atoval}@um.es

Abstract. A number of cloud applications are currently widely used. However, one of the main reasons for the slowing down in the growth of cloud computing is that of security. Even though some research has been done in the security field, it is necessary to assess the current state of research and practice. This paper aims for the study of the existing research about security in cloud computing to analyze the state of art and to identify future directions. The method selected to investigate the security in cloud computing is a systematic mapping study. A total of 344 papers were selected and classified by security goal, research type and contribution type. The main security specific issues extracted are data protection (30.29%), access management (20.14%), software isolation (16.70%), availability (16.00%), trust (13.60%) and governance (3.27%). Our results demonstrate that cloud computing seems to be a promising area for security research and evaluation.

Keywords: cloud computing, security, mapping study.

1. Introduction

The US National Institute of Standards and Technology (NIST) describes Cloud Computing, from now on CC, as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." [1]. Many cloud applications are currently widely and successfully used (i.e. Google App Engine, Amazon's Computer Cloud Amazon Web Service and Microsoft Azure Service Platform). Although CC is a growing technology, no key player leads this revolution. The cloud saves money and has the backing of many large software vendors [2]. However, one of the main reasons why the growth of CC has slowed down is that of security, which is the greatest challenge of CC [3]. A few examples of this type of threats are two real incidents that occurred in 2009. One of them is Salesforce.com, which suffered an outage that locked more than 900,000 subscribers out of crucial CC applications and data needed to transact business with customers [4]. Another example is that of the smartphone known as "Sidekick" when users (over 800,000) temporarily lost personal data, which was accessed as a cloud service [5].

CC systems are secure if users can depend on them to behave as would be expected. Security in terms of information security is a condition that results from the establishment and maintenance of protective measures that enable an enterprise to

perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery and correction that should form part of the enterprise's risk management approach [6]. 5 goals have traditionally been associated with the achievement of adequate security: availability, confidentiality, data integrity, access control and audit [7]. The National Institute of Standards and Technology (NIST) has published the Guidelines on Security and Privacy in Public Cloud Computing, which provides an overview of the security and privacy challenges pertinent to public CC and points out considerations that organizations should bear in mind when using the cloud environment [8].

Despite the research that has been carried out in the field of CC security, it is necessary to assess the current state of research and practice in order to provide practitioners with evidence that will enable them to focus on its further development. The method selected to investigate the state-of-the-art is a systematic mapping study. A systematic mapping study provides an objective procedure with which to identify the nature and extent of the research that is available to answer a particular research question. These kinds of studies also help to identify gaps in current research in order to suggest areas for further investigation. Some surveys summarize risks and recommendations but do not follow procedures for a systematic mapping study [9] [10].

Silva et al. [11] performed a mapping study that focuses on accounting models for CC, classifying them into three categories: contribution type, research type and accounting models features. They provide an overview of the area, in addition to specific findings related to the taxonomy for accounting process, accounting models, pricing schemes and SLA (Service-Level Agreement) composition. The analysis done in [12] examines the different existing approaches in the literature about migration processes to CC while taking into account the security aspects that have to be also moved to Cloud. The review of cloud security proposals developed by Rebollo et al. [13] compare existing information security frameworks that have been specifically designed for the CC environment using the clauses from the ISO/IEC 27002 standard as evaluation criteria. The same authors also conduct a systematic literature review [14] to extract existing Information Security Governance frameworks that are suitable for application in CC. To the best of our knowledge, no systematic mapping study on security in CC currently exists.

The aim of this paper is therefore to study the existing research concerning security in CC in order to analyze the state-of-art and to identify future directions. The method consists of the application of a systematic mapping study to extract as much literature as possible. The 344 papers selected have been classified by their security goal, research type and contribution type.

The article is organized as follows: Section 2 shows how the mapping study was planned by defining the research questions and describing how the review was carried out: search strategy, inclusion and exclusion criteria and classification scheme. Section 3 synthesizes the results obtained by answering the research questions raised. In Section 4 we discuss the findings of our research and present the limitations of the study. Finally, in Section 5 we draw our conclusions.

2. Mapping Study

According to Petersen et al. [15], a systematic mapping study provides a structure of the type of research reports and results that have been published by categorizing them. It often provides a visual summary, a map, of its results. A number of research questions must be defined in order to obtain these objectives in a systematic manner. The main goals of a structured mapping study are to present an overview of a certain research area and to identify research gaps.

A systematic literature review is another kind of secondary study that answers specific research questions by identifying, analyzing and interpreting relevant evidence. A systematic mapping study, unlike a systematic literature review, does not analyze the articles identified in detail [15].

Petersen et al. propose five process steps when performing a systematic mapping study [15]. In the first step, the research questions are developed in order to define the scope. The next two phases include searching for and selecting primary studies by screening the articles found. The data is then extracted and synthesized. In a last phase the review results are obtained and the research questions are answered.

2.1. Research Questions and Search Strategy

The principal goal of this study is to analyze publications concerning the security in CC. This overall goal is defined in four research questions. Table 1 shows these research questions along with their motivation.

The main digital libraries used to search for primary studies were: IEEE Digital Library, IEEE-Xplore, ACM Digital Library, Science Direct and Wiley InterScience. These publication databases were chosen since they are some of the most relevant sources in software engineering.

Petersen et al. recommend defining the search string by using the PICO criteria: population, intervention, comparison and outcome. They also state that it should be driven by the research questions. When defining a search string, the resulting set should have the maximum possible coverage, but should also be of a manageable size. As the research questions suggested, a broad overview of the research area was desired, and some restrictions, such as temporal restrictions or specific security areas restrictions were therefore avoided in order to construct a complete map. In addition to the selected terms, boolean operators were used to form the complete search string which is composed of three parts. In the ACM Digital Library this search string is defined as:

"cloud computing" AND
("security" OR "risk" OR "vulnerability" OR "threat")
AND Title: "cloud".

The search process took place from November 2012 to December 2012. This process was conducted by applying the same search string to the same meta data (title or complete text) of each article for all the sources, although the search string's syntax was adapted to each digital library. A restriction on publication date was not established, but the papers obtained had all been published in the last few years.

Table 1. Research questions.

No.	Research question	Motivation
RQ1	What are the main security areas investigated in cloud computing?	The first research question defines the basis of this systematic mapping study and provides an overview of recent studies.
RQ2	What kinds of research and contributions have been proposed?	This question provides information about the concrete techniques and solutions that have been proposed.
RQ3	How publications have evolved over time? What are the research and publication trends?	The third question shows the evolution of the publications concerning the subject under study.
RQ4	In which bibliographical sources were they published?	This last question examines the different sources in which the articles concerning security in CC are published.

2.2. Screening of Papers for Inclusion and Exclusion

The aim of the selection process was to identify those articles that are most relevant for the objective of this mapping study. Each study that was retrieved from the previous search was evaluated in order to decide whether or not it should be included by considering its title, abstract and keywords.

The studies that met at least one of the following inclusion criteria were included:

- Studies reporting some topic related to security in CC.
- Studies presenting actual security risks in CC.
- Studies proposing a solution in order to guarantee security in CC.

The following studies were excluded from the search results:

- Studies reporting a particular topic related to CC but not security in CC.
- Studies that mention security in CC but in a superficial manner.
- Studies concerning CC technology applied to a concrete application.
- Studies concerning security in CC but from a legal perspective.
- Studies concerning security in CC but from a business perspective.

The search phase obtained a set of 1757 papers, most of which were found in the IEEE Digital and ACM Digital libraries. As shown in Fig. 1, 500 articles were considered based on article title and on the inclusion and exclusion criteria. In the second phase, 84 duplicated studies were removed, resulting in 416 articles being included in the next phase. In the third phase, 72 articles were discarded and 344 were selected based on the abstract and the sub-section titles. The number of selected articles that remained was 344. The complete list of selected articles can be downloaded from [16].

The following step in the study was to read all the abstracts in order to assign keywords to each paper. With some papers, it was necessary to read the introduction, conclusion or even section titles to be able to extract these keywords.

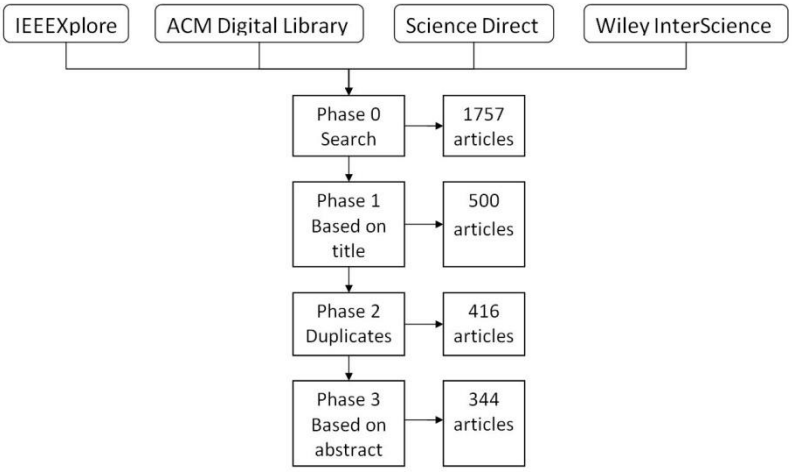


Fig. 1. Selection process of primary studies.

2.3. Classification Scheme

The classification scheme proposed in this paper was adapted from Petersen et al. [15], with the exception of the Security Goal facet that was obtained from the NIST Guidelines on Security and Privacy in Public Cloud Computing [8]. The scheme consists of three facets: security goal, research type and contribution type (see Fig. 2). Classification schemes are rated on the basis of a set of quality attributes [17]:

- Orthogonality. There are clear boundaries between categories, which makes it easy to classify.
- Defined based on existing literature. The taxonomy/classification is created on the basis of an exhaustive analysis of existing literature in the field.
- Based on the terminology used in literature. The taxonomy uses terms that are used in existing literature.
- Complete. No categories are missing, thus allowing existing articles to be classified.
- Accepted. The community accepts and knows the classification/taxonomy.

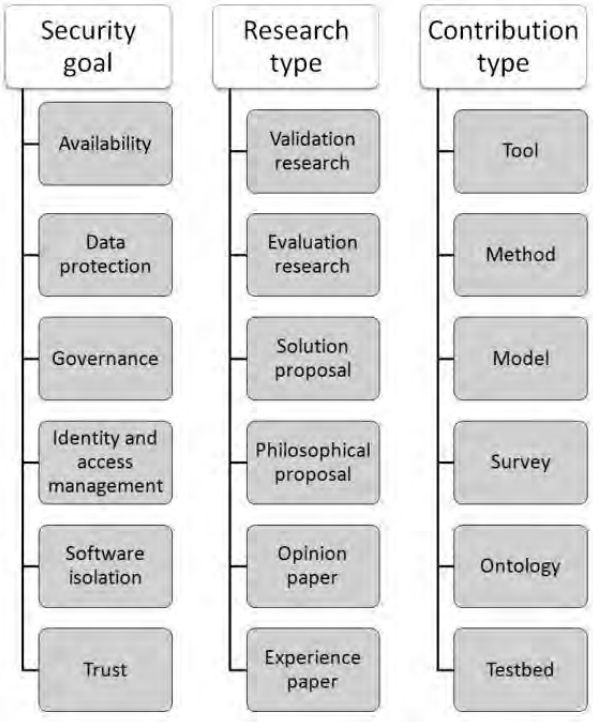


Fig. 2. Facets.

Security goal

There are different approaches for classification of security aspects in cloud computing. Fernandes et al. [18] propose a taxonomy that covers eight categories: software, storage and computing, virtualization, Internet and services, network, access, trust, and compliance and legality. Gruschka and Jensen [19] present a taxonomy for attacks on cloud services. The ISO/IEC DIS 27017 [20] is a standard in progress, which is being specifically tailored to cloud services and defines guidelines to support the interpretation and implementation of cloud-specific information security controls supplementing the guidance in ISO/IEC 27002. The ISO 27799, an implementation of ISO/IEC 27002 in health informatics [21] [22], has been already used in secondary studies [23] [24]. The Security goal facet used in this article is based on the NIST Guidelines on Security and Privacy in Public Cloud Computing [8], which is a publication accepted by the community in the field. This facet includes six categories based on different key security and privacy issues identified by NIST (see Table 2).

The 4.2 section of the guidelines is about compliance. Compliance is the company responsibility to operate in agreement with established laws, regulations, standards and specifications, so as it was mentioned in the exclusion criteria, compliance is out of this study bounds. Section 4.4 about the architecture is really distributed among the rest of

the categories; due to the proposed architectures can have the objective of protecting data, ensuring the availability or keeping the software isolation.

- Governance. Governance implies control and oversight by the organization over policies, procedures and standards for application development and information technology service acquisition, as well as the design, implementation, testing, use and monitoring of deployed or engaged services [8].
- Trust. Trust in the cloud can be viewed as the customers' level of confidence in using the cloud. Confidence can be increased by mitigating technical and psychological barriers to using cloud services [25].
- Identity and access management. This category includes the identity proofing and authentication aspects, and the prevention of unauthorized access to information resources in the cloud [8]. Access control systems provide identification and authentication services (who can log on), authorization (what a subject can do) and accountability (what a subject did) [6].
- Software isolation. High degrees of multi-tenancy over large numbers of platforms are needed for CC to achieve the envisioned flexibility of on-demand provisioning of reliable services and the cost benefits and efficiencies due to economies of scale. Multi-tenancy in IaaS (Infrastructure as a Service) CC environments is typically done by multiplexing the execution of virtual machines from potentially different consumers on the same physical server [8]. Virtualization is the simulation of the software and/or hardware upon which other software runs. This simulated environment is called a virtual machine (VM) [26].
- Data protection. Data stored in the cloud usually resides in a shared environment with data from other customers. Organizations moving sensitive data into the cloud must account for the means by which access to the data is controlled and is kept secure [8]. Papers which describe measures to ensure data protection and data security, in particular data confidentiality and integrity are classified in this category.
- Availability. This category refers to the availability of information resources and may be affected by technical issues, natural phenomena or human causes. The dynamic provisioning of a cloud simplifies the work of an attacker to cause a denial of service. Papers that describe investigations concerning availability in CC are mainly solutions with which to avoid denial-of-service attacks [6] [27].

The security categories are not mutually exclusive so that one paper can discuss both availability and data protection issues. The keywords used to classify the papers into these categories are listed in Table 3.

Table 2. Association between categories, NIST Guidelines on Security and Privacy in Public Cloud Computing and security elements

Category/Guidelines section	Security element
4.1 Governance	Audit
4.3 Trust	Audit
4.5 Identity and Access Management	Access control
4.6 Software isolation	Integrity, Confidentiality
4.7 Data Protection	Integrity, Confidentiality
4.8 Availability	Availability

Table 3. Keywords for security goal

Security Goal	Keywords
Availability	denial of service, intrusion, attack, malware, detection, infrastructure
Data protection	data protection, integrity, confidentiality, privacy, encryption
Governance	governance, policies, procedure, standard, requirement, rule
Identity and access management	identity, access, privilege, authentication, key, cryptography, certificate
Software isolation	software isolation, multi-tenancy, virtualization, virtual machine (VM), hypervisor, environment
Trust	trust, risk management, transparency, credibility, reliability, data location, monitor

Research type

The research type facet is based on the schema proposed by Wieringa et al. [28]. This facet has six categories. The keywords used to classify the papers into these categories are listed in Table 4.

Table 4. Keywords for research type

Research type	Keywords
Validation research	test, result, simulation, emulator, analysis, experiment, prototype
Evaluation research	evaluation, implementation, result, platform, case study, production
Solution proposal	solution, proposal
Philosophical paper	philosophical paper
Opinion paper	discuss, survey, suggests
Experience paper	experimental

- Validation research. A validation research has not been implemented in practice and focuses on the validation of the solution in the lab or in CC simulation scenarios. Validation studies should include discussions concerning limitations. A CC validation research states hypotheses, uses summary statistics and describes the main components of an experimental setup.
- Evaluation research. Evaluation research has been implemented in practice and shows the solution implementation and what the consequences of the implementation in a CC environment are in terms of benefits and drawbacks. Evaluation research can be excluded if no industrial cooperation or real world project is mentioned.
- Solution proposal. A solution proposal is a new technique or a significant extension to an existing one. Its benefits are exemplified or argued, but there is no complete validation in a CC environment.
- Philosophical proposal. This proposal shows a point of view as regards the subject without the preciseness of a solution proposal. These papers sketch a new way of looking at existing things by structuring the field in the form of a taxonomy or conceptual framework.

- Opinion paper. An opinion paper reports the author's opinion of what is good or bad. In this study, opinion papers are those in which the author carries out a theoretical study or proposes CC security recommendations.
- Experience paper. An experience paper reports on personal experiences from a real life CC project. Research methodology is not included.

Contribution type

These categories are extracted from Petersen's article [15]. They have been slightly adapted to CC security through, for example, the creation of the ontology category. An ontology represents the vocabulary of a domain, therefore, for a recent discipline as CC, it should be common to create ontologies to clarify the structure of knowledge [29]. The keywords used to classify the papers into these categories are listed in Table 5.

- Tool. Papers proposing a tool related to CC. A privacy manager or a decision support tool, are some examples of this.
- Method. Papers describing a new method. Encryption methods, secure protocols (such as non-repudiation protocols) or communication protocols were identified as methods.
- Model. Papers proposing models such as system architectures or CC frameworks (in the sense of an architecture framework, not a software framework).
- Survey. Papers exposing risks and vulnerabilities in CC, but in which no solution is proposed.
- Ontology. Papers proposing an ontology to identify and discuss the information that will be exchanged in order to preserve security in CC.
- Testbed. Papers proposing a testbed that enables researchers to study different aspects of CC.

Table 5. Keywords for contribution type

Contribution type	Keywords
Tool	tool, demo, implementation, manager, execution
Method	method, mechanism, technique, protocol, algorithm
Model	model, framework, architecture, implementation, system, scheme
Survey	survey, categorizes, recommendation, best practices
Ontology	ontology, property, connection
Testbed	testbed, evaluate, debug

3. Results

Each article was classified into the categories of each facet in order to answer the four research questions. The results of the systematic mapping study are presented as follows.

3.1. RQ1: What are the main security areas investigated in cloud computing?

In order to be able to answer this question, the security goal facet was created. Its results are shown in Table 6. Most of the papers deal with data protection (30.29%), followed by identity management (20.14%), software isolation and availability with very similar percentages (16.70% and 16.00%), trust (13.60%) and the least studied topic is that of governance (3.27%).

199 of 344 papers (57.85%) discuss about just one topic at a time and just the NIST guidelines include all the security issues [8]. Those 199 papers keep similar percentages for the different categories so that they imply the major contribution to the global ranking: 75 are about data protection, 44 about identity management, 28 about software isolation, 28 about availability, 18 about trust and 6 about governance.

Data protection is related to privacy, integrity and confidentiality topics. To achieve data protection authors address privacy managers, encryption schemes (34 papers), audit practices (16 papers), noise generation strategies (5 papers) or storage methodologies (4 papers). For example, Cachin et al. surveyed some cryptographic tools and concluded that these kinds of solutions are academic and should be evaluated in practice [30]. With regard to noise generation strategies, Zhang et al. [31] propose a strategy based on historical probability as a means to reduce the number of noise requests. One example of the use of storage methodology to maintain data secure is that described by Subashini et al., which consists of a fragmentation technique based on the sensitivity and value of the data [32].

Identity management is covered in its most by access control architectures, even so, alternative issues can be found such as watermarking methods, authentication frameworks or encryption schemes. Software isolation is done by virtualization techniques. Availability involves intrusion and DoS (Denial-of-Service) attack detection systems and audit practices, such as [33] et al. that offer a solution to detect the source of a DoS attack and filter the attack traffic.

Table 6. Number of papers by security goal

Security goal	Number of papers	Percentage
Data protection	176	30.29%
Identity and access management	117	20.14%
Software isolation	97	16.70%
Availability	93	16.00%
Trust	79	13.60%
Governance	19	3.27%

3.2. RQ2: What kinds of research and contributions have been proposed?

Upon examining the contribution type facet results in Table 7 it was discovered that most of the solutions are model proposals, that is, secure architectures for CC systems. Some examples are presented to illustrate the utility of these architectures. Zhang et al. [34] who present an information risk management framework in order to better understand critical areas of focus in a CC environment. This framework also helps as

regards identifying threats and vulnerabilities. Lin and Squicciarini [35] propose a new data protection framework that addresses challenges during the life cycle of a CC service. This framework consists of three key components: policy ranking, policy integration and policy enforcement. With regard to dataflow processing, Juan Du et al. present ROSIA, a robust service integrity attestation system whose purpose is to process stateful dataflow applications in CC [36]. There is also a framework proposal for mobile environments. Jarabek et al. [37] develop a cloud-based anti-malware system for Android. Performance and data consumption of this system is then evaluated using 50 Android applications downloaded from Google Play market.

Table 7. Number of papers by contribution type

Contribution type	Number of papers	Percentage
Model	143	41.57%
Method	96	27.91%
Survey	92	26.74%
Tool	7	2.03%
Ontology	5	1.45%
Testbed	1	3.27%

96 out of 344 papers propose methods (27.91%). The methods are secure communication protocols, cryptographic algorithms with which to encrypt data and measures to detect problems in system integrity or to measure the trustiness of the cloud resources. Some representative papers selected to show the goal of these methods are Kwon et al. and Wang et al.; Kwon et al. [38] propose measures to detect anomalies or abnormal activities. Wang et al. [39] propose a method to efficiently share confidential data on cloud servers by combining the hierarchical identity-based encryption system and the ciphertext-policy attribute-based encryption system. Zhang et al. [40] propose an integrity verification scheme that allows a third party auditor to verify the integrity of multiple stored replicas.

Around 26.70% of the papers are surveys. These papers are theory studies in which the actual situation of CC is explained. Some also make recommendations, such as Dahbur et al. [9] who make the necessary hints that can help promote the benefits of and mitigate the risks associated with CC. Hay et al. [41] suggest some future directions for security research and development to help advance the security posture of this technology.

Table 8. Number of papers by research type

Research type	Number of papers	Percentage
Solution proposal	134	38.95%
Validation research	107	31.10%
Opinion paper	83	24.13%
Evaluation research	13	3.78%
Philosophical paper	6	1.75%
Experience paper	1	0.29%

Only 7 papers propose a tool (2.03%). One of the first tools published was a client-based privacy manager that helps reduce the risk of data leakage or loss of privacy, and

provides additional privacy-related benefits by reducing the amount of sensitive information sent to the cloud [42]. D. Tancock et al. [43] propose the Privacy Impact Assessment (PIA) decision support tool that can be integrated within a CC environment. There are another 5 papers that create an ontology or taxonomy, and a further one which proposes a test bed [44].

Regarding the research type facet in Table 8, 38.95% of the papers are solution proposals, i.e., solutions that have not been evaluated in real practical scenarios. Solutions validated in experiments or prototypes represent around 31.10%, while evaluation research papers represent around 3.78%. In evaluation research, the solution has been implemented in practice, while the experiments validate the solution in the lab or in simulation scenarios. Of 13 evaluation papers, only 4 are case studies. To better understand the contribution of the papers located in these categories, some representative examples are provided. Balduzzi et al. conduct the evaluation of a real system [45], in which the security problems of public images that are available on the Amazon EC2 service are investigated. Lo et al. [46] propose a framework of cooperative intrusion detection system (IDS) to reduce the impact of denial-of-service (DoS) attack or distributed denial-of-service (DDoS) in a CC environment. The authors validate the proposed system with experimental results that indicate that the framework could resist DoS attack. Dhage et al. [47] propose an architecture capable of detecting intrusions in a distributed CC environment and safeguarding it from possible security breaches, but no validation results are mentioned.

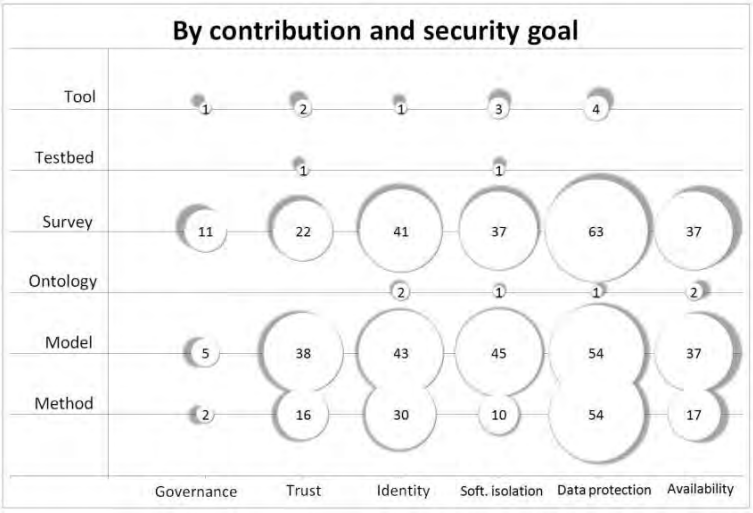


Fig. 3. Number of papers by contribution and security facets.

Opinion papers represent around 24.13% (83 papers). These papers are reviews of security that provide personal recommendations. They are closely related to surveys from the contribution type facet. The remaining 1.75% of the studies belongs to philosophical papers. Only one experience paper has been found [48]. In this paper, Oza et al. identify and marry a range of issues related to user experience and security.

Some additional graphics have been created to allow the relations between the facets to be observed. The goal security facet is compared in Fig. 3 and Fig. 4. Most of the papers belong to the data protection category and most of them are solution proposals

and opinion papers, respectively. Fig. 5 represents the contribution type and investigation type facets.

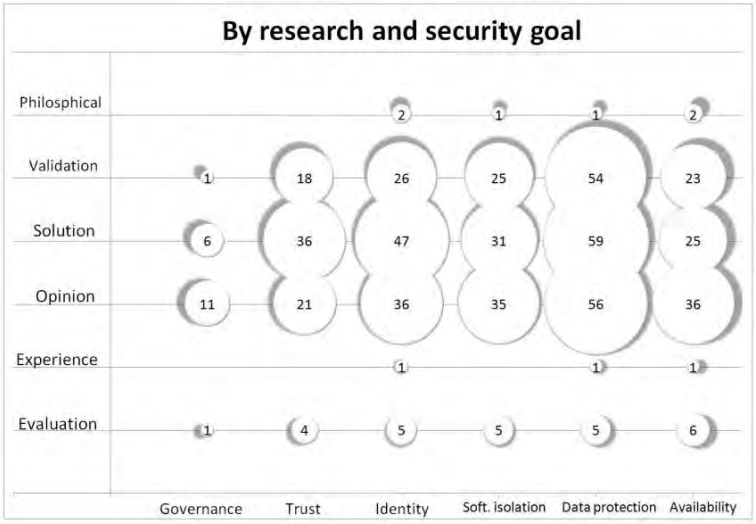


Fig. 4. Number of papers by research and security facets.

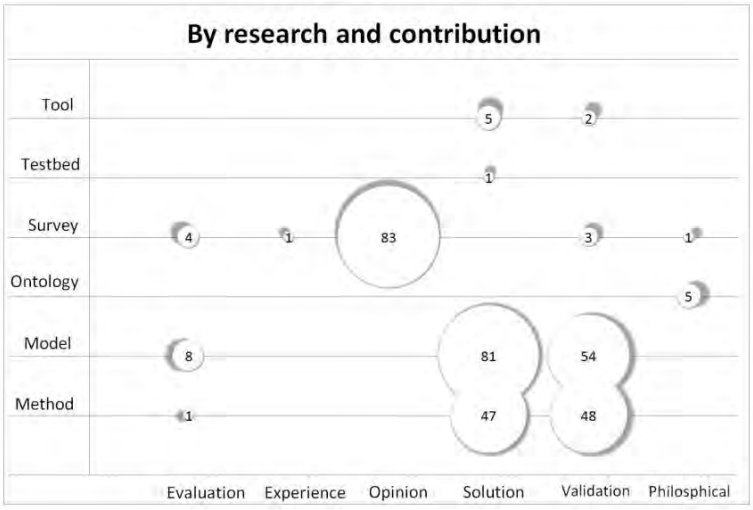


Fig. 5. Number of papers by research and contribution facets.

3.3. RQ3: How have publications changed over time?

Four different years could be identified, 2009, 2010, 2011 and 2012. More than 40% (139 articles) of the articles was published in 2012. Fig. 6 and Fig. 7 show the distribution of the papers by year. The evolution of publications by research type (see Fig. 7) is the same as the general evolution (see Fig. 6), the number of papers gets

bigger and bigger, doubling each year. This fact is observed in almost every single category: validation research, solution proposals, philosophical papers, opinion papers and evaluation research.

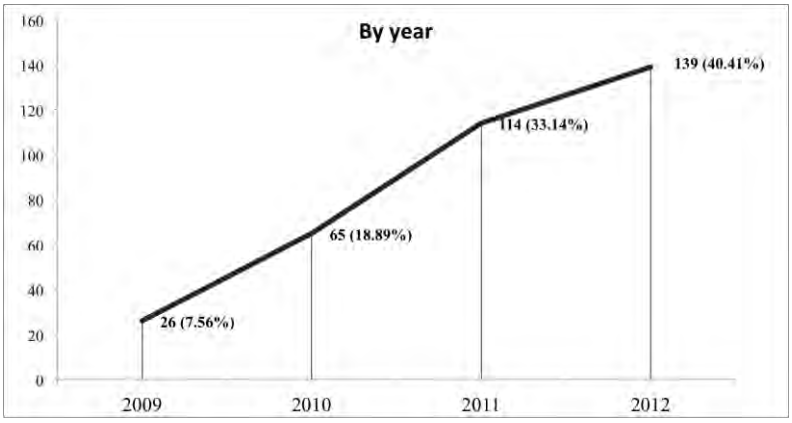


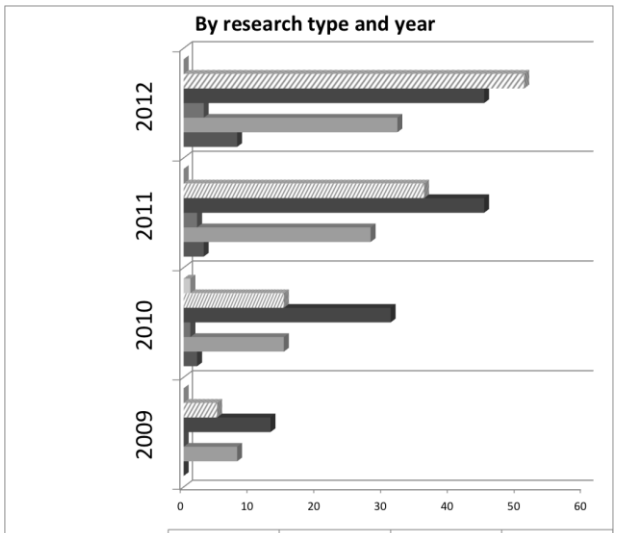
Fig. 6. Number of papers by year.

3.4. RQ4: In which sources were they published?

This question is answered by extracting the conference or the journal in which the papers were published. The Journal Citation Report (JCR) has been used to evaluate the recognition and stability of a journal with a systematic and objective system. JCR is an evaluation mechanism based on statistic information from reference data. The Computing Research and Education (CORE) system has been used to evaluate conferences. This is a Computing Research and Education Association of Australasia ranking mechanism.

More than 73.26% of the articles (252 articles) were presented at conferences and 23.84% of them were published in journals. The remaining articles were not published in either conferences or journals, but rather in books. Note the variety of different publishing sources: 132 conferences and 40 journals were identified.

In the journal ranking, the top one is IEEE Security and Privacy together with Future Generation Computer Systems: 9 papers. The next, with 6 papers, is the Journal of Computer Law and Security Review, but most of the remaining journals have just one or two selected papers. In the conference ranking, the top one is CLOUDCOM with 26 papers. CCSW is in second position with 11 papers; and DASC is in third position with 9 papers.



	2009	2010	2011	2012
Experience paper	0	1 (1.54%)	0	0
Validation research	5 (19.23%)	15 (23.08%)	36 (31.58%)	51 (36.69%)
Solution proposal	13 (50%)	31 (47.69%)	45 (39.47%)	45 (32.37%)
Philosophical paper	0	1 (1.54%)	2 (1.76%)	3 (2.16%)
Opinion paper	8 (30.77%)	15 (23.08%)	28 (24.56%)	32 (23.02%)
Evaluation research	0	2 (3.08%)	3 (2.63%)	8 (5.76%)

Fig.7. Number of papers by year and research type.

4. Discussion

The current situation of security in CC has been analyzed by examining the research and new advances published. Based on the results of this systematic mapping study, the first finding is that CC is a recent discipline since the papers found were only published in 2009, 2010, 2011 and 2012. Moreover the fact that not many papers report on tools or solutions evaluated in real scenarios (2.03% and 3.78%) also demonstrates this statement. Validations (31.10%) by way of experiments are more frequent than evaluations (3.78%) that involve case studies or implementations, but the most common research type consists of solution proposals, which only provide the scenario and direction of the solution. Case studies represent only 1.16% of papers. This situation is particularly critical for security in CC [49] [50] since conducting and examining real-world case studies allows best practices for CC to be learnt and established [51]. These results coincide with those of authors who describe CC as a new technology [52]. CC has gained increased attention during the past three years, and would appear to be a promising area for further research [10].

Each year the number of papers increases but the growth rate is lower (Fig. 6). The number of papers published in 2009 increased by 150% in 2010, by 75% from 2010 to 2011 and by 22% from 2011 to 2012.

We performed a regression analysis on this data and found there is a strong positive correlation between year and the number of publications. In order to predict the trend of

publications in the future, we have tried to determine a trend line for this data using several common regression models: Linear, Logarithmic, Polynomial, Power, Exponential and Moving average. The quadratic model is the best-fit line we found, which achieves a coefficient of determination of $R^2 = 0.9924$. To put the CC growth trend into a wider context, according to DBLP (Trier Universität, 2012), the general growth in computer science is exponential. Fitting an exponential model to our data, a coefficient of $R^2 = 0.9238$ is obtained.

Upon extracting the evolution of the research type over the years, some interesting information can be found (Fig. 10). The proportion of papers that only propose solutions has decreased: 50% (2009), 47.69% (2010), 39.47% (2011) and 32.37% (2012). Instead, validation research papers have increased over the years: 19.23% (2009), 23.08% (2010), 31.58% (2011) and 36.69% (2012). This provides some evidence to suggest that the CC is starting to move from foundational theory to practical validation, possibly a sign of puberty.

Of all the extracted security-related topics, data protection is that which is most frequently studied, owing to the fact that a significant barrier to the adoption of cloud services is the fear of leakage of sensitive data or loss of privacy [42]. Ponemon Institute conducted a study about security in CC in which 925 IT practitioners from US and Europe were surveyed in 2010 [54]. One of the results of this study was the rating from respondents who said they were confident that their organizations could achieve some security features. The security feature with the least confidence percentage was *Secure sensitive or confidential information at rest* (33%) which explains the great interest in studying data protection. The next security features with low confidence percentages were: *Prevent or curtail external attacks, Secure vendor relationships before sharing information assets* and *Identify and authenticate users before granting access to information assets or IT infrastructure*. This last one can be mapped to our identity and access management category, the second one in our results.

In contrast, relatively little attention (3.27% of the papers) has been paid to the governance in CC. Our finding also confirms the study performed by the Ponemon Institute, in which respondents identified governance as one of the least important technology to securing CC. In a follow-up study performed in 2012 [55] which goal was to determine what changes had occurred in the respondents answers since the first study [54], the results showed that there was no clear answer according to respondents about who should ensure the security of IaaS, so the authors suggested that it is important to improve governance by establishing responsibilities and policies that define the process of checking the CC security.

Trust is the next one with a low number of papers (13.60%), but unlike governance, trust is a key element to the real users of a CC system. The only experience paper extracted from this mapping study presents an analysis of user experience issues in CC [48]. The analysis was conducted by Nilay Oza et al. using an interview process. The 100% of the interviewees mentioned trust as one affector of their user experience. The confidence in a cloud service provider depends on factors such as the presence in social networks, friend referrals, position in search engines, language or cost of the service. These indicators are just a starting point. In fact the real service will build the confidence level of the provider. The confidence level depends on the security controls to protect the data and applications. Audits performed by third-parties may play a key role in achieving a minimum level of trust [8]. Our findings present 15 articles about audit, contributing with models, methods, surveys but just one of them is a tool. This

demonstrates the absence of audit reporting tools and, in general, CC specific tools, as Bryan Doerr also suggests [56].

From a practitioner's point of view, the results presented in this study provide an overview of existing security approaches in CC. This technology has not yet reached great levels of expansion, which provides new opportunities for innovation. The approaches and models proposed are in their beginnings and should be applied to real systems. Around 42% of contributions are proposals for new models and only 5.59% of them are evaluated. Working with existing CC security frameworks should be considered. The NIST, which has published the Guidelines on Security and Privacy in Public Cloud Computing [8], has also defined the NIST Cloud Computing Security Reference Architecture [57]. This architecture introduces a Risk Management Framework for applications or services in the cloud. The comparative criteria proposed by Rebollo et al. [14] could be adopted in order to analyze and compare CC related frameworks. This comparative framework includes the following characteristics: *Policies and Processes Adaptation*, *Control and Audit*, and *Service Level Agreements*.

From a researcher's point of view, multiple lines of investigation emerge as a result of the few years of experience in CC. Even the term 'cloud computing' itself is still vague, with no universal definition [58]. The main line of investigation focuses on studying more specific security mechanisms, such as audit, and on evaluating the solutions and proposing stable models and methodologies which are capable of tackling the real world problems in CC. 38.95% of the papers are solution proposals that have not been evaluated in real practical scenarios, which demonstrates that CC is a recent research field. There is a need for research on evaluation, and likewise experience papers and tools (only 7 papers propose a tool, 2%).

Alternative solutions are also required, such as ontology definitions, or software test suites, both of which are unexplored fields. Ontologies are the first step to perform an analysis of the domain. Having more articles proposing ontologies will enable knowledge sharing [29] and therefore facilitate the creation of missing universal terminology of CC. In this mapping study, just one paper proposing a testbed was found, the Open Cirrus Testbed [44], but there are some other important non-published testbeds: PlanetLab [59], EmuLab [60], IBM-Google NSF CluE [61], Amazon Cloud [62], Eucalyptus Public Cloud [63], Open Cloud Testbed (OCT) [64], VINI [65] or OneLab [66]. Our study shows the lack of articles about the use of testbeds and the lack of citations to these providers. A testbed in cloud computing is a network platform available to researchers and developers for experimentation, to develop, debug and evaluate their systems [60]. Since researchers have to validate and evaluate their solution proposals, testbeds can help them with that task. Nevertheless, notice that testbeds are emulators that are not entirely representative of the Internet [67].

4.1. Limitations of the Study

There is a set of threats to validity.

- Conclusion validity. Conclusion threats to validity in a mapping study are related to incorrect data extraction or missing studies [68]. One limitation of this systematic mapping study is the distortion of statistical analysis owing to the criteria used in the selection phase. The final results depend on the decisions made by the researcher who conducted the search process. This limitation was alleviated by defining the

inclusion and exclusion criteria in order to assemble the most extensive amount of papers conforming to the domain. In the steps of selecting and classifying, bias may affect the interpretation of the results. This limitation was alleviated by clearly describing every activity performed in these steps.

- Construct validity. Construct threats to validity in a mapping study are related to the identification of primary studies [69]. Security in CC is a wide topic and requires the consideration of more specific research questions, since the goal of systematic mapping studies is more oriented towards categorizing the papers selected. Different terms related to security (i.e privacy, vulnerability or risk) were determined in order to find a wide range of articles. However, the results found could not be complete due, either to the manual research or the fact of missing other terms in the search string, which could has affected the final list of articles selected. To alleviate this threat, the PICO criteria was used and different terms were added to the search string. The search for primary studies was performed by using IEEE Digital Library, IEEE-Xplore, ACM Digital Library, Science Direct and Wiley InterScience. According to Zhang et al. [70], IEEE Xplore and ACM Digital Library are the main search portals in software engineering.
- Internal validity. Internal threats to validity in a mapping study are related to the extraction and data analysis [69]. A common view is that mapping studies are often conducted based on only the abstracts. However, we have detected that in the search and inclusion/exclusion phase, the extraction of relevant information was particularly difficult owing to the fact that some abstracts are often misleading and lack important information. Structured abstracts, which ensure that all important information is available such as background, research method and conclusions would help in the identification of studies [71]. This threat was alleviated by additionally allow more detailed study of papers for which it is not clear how they should be classified. The more parts of a paper one considers, the more effort is required and the validity of the results also increases [15]. Data extraction could also result in a misclassification, but this limitation was alleviated by creating a classification scheme on the basis of widely accepted guidelines [26].
- External validity. External threats to validity in a mapping study are related to the generality of the results [72]. The validity of the conclusions drawn in this paper concerns only this systematic mapping study. This threat is therefore not present in this context.

5. Conclusions

Various relevant conclusions have been extracted from this systematic mapping study, which provides a structure of the type of research reports, and results that have been published as regards security in CC. Different security issues are being investigated: data protection, access management, software isolation, availability, trust and governance. Most of the solution proposals are models, followed by methods. The proposed solutions are secure architectures for CC systems, communication protocols and encryption protocols. Although the first year of publication was 2009 and the number of publications would appear to be growing, 40.00% of the papers are proposals that do not contain any real evaluations and around 26.74% are surveys that contain no

proposals at all. The idea of CC as an emerging technology is supported by these results, thus creating a favorable area for research and evaluation, with special emphasis on security [73].

The total of 344 papers selected were found in a variety of 172 different publishing sources, signifying that this topic is the source of a huge amount of interest in different fields of computer science. Other disciplines such as health [74], business [75] [76], and education [77] [78], among others, are also important application areas in which a strong growth of publications is expected. The secure use of cloud services through mobile devices [79] and the security assurance mechanisms in green cloud computing environments [80] are also promising research areas.

Acknowledgements. This research is part of the projects PEGASO-PANGEA (TIN2009-13718-C02-02) financed by the Spanish Ministry of Science and Innovation (Spain), and GEODAS-REQ project (TIN2012-37493-C03-02) financed by both the Spanish Ministry of Economy and Competitiveness and European FEDER funds.

References

1. Mell, P., Grance, T.: The NIST Definition of Cloud Computing. Tech. rep. (2009) Available at http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.
2. Lillard, T., Garrison, C., Schiller, C., Steele, J.: The Future of Cloud Computing. In Lillard, T., Garrison, C., Schiller, C., Steele, J., eds. : Digital Forensics for Network, Internet, and Cloud Computing 12. Elsevier, Syngress, Boston (2010) 319-339
3. Modi, C., Patel, D., Borisaniya, B., Patel, A., Rajarajan, M.: A survey of intrusion detection techniques in Cloud. Journal of Network and Computer Applications 36(1), 42-57 (January 2013)
4. Ferguson, T.: Salesforce.com outage hits thousands of businesses. (Accessed 2009) Available at: http://news.cnet.com/8301-1001_3-10136540-92.html
5. Cellan-Jones, R.: The Sidekick Cloud Disaster. (Accessed 2009) Available at: http://www.bbc.co.uk/blogs/technology/2009/10/the_sidekick_cloud_disaster.html
6. Kissel, R.: Glossary of key information security terms [electronic resource]. (Accessed 2006) Available at: http://permanent.access.gpo.gov/lps80291/NISTIR-7298_Glossary_Key_Infor_Security_Terms.pdf
7. Zhou, M., Zhang, R., Xie, W., Qian, W., Zhou, A.: Security and Privacy in Cloud Computing: A Survey. In : Proceedings of the 2010 Sixth International Conference on Semantics, Knowledge and Grids, Washington, DC, USA, pp.105-112 (2010)
8. Karen, M., Hoffman, P.: Guidelines on Security and Privacy in Public Cloud Computing. Tech. rep. (December 2011) Draft Special Publication 800-144. Available at http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909494.
9. Dahbur, K., Mohammad, B., Tarakji, A.: A survey of risks, threats and vulnerabilities in cloud computing. In : Proceedings of the 2011 International Conference on Intelligent Semantic Web-Services and Applications, New York, NY, USA, pp.12:1-12:6 (2011)
10. Zissis, D., Lekkas, D.: Addressing cloud computing security issues. Future Generation Computer Systems 28(3), 583-592 (2012)
11. Airton Pereira da Silva, F., da Mota Silveira Neto, P., Cardoso Garcia, V., Elia Assad, R., Mota Trinta, F.: Accounting Models for Cloud Computing: A Systematic Mapping Study.

Proceedings of the 8th International Conference on Grid Computing and Applications (GCA), 3-9 (2012)

12. Rosado, D., Gómez, R., Mellado, D., Fernández-Medina, E.: Security Analysis in the Migration to Cloud Environments. Future Internet 4(2), 469-487 (2012)
13. Rebollo, O., Mellado, D., F-Medina, E.: A Comparative Review of Cloud Security Proposals with ISO/IEC 27002. In : Proceedings of the 8th International Workshop on Security in Information Systems, pp.3-12 (2011)
14. Rebollo, O., Mellado, D., F-Medina, E.: A Systematic Review of Information Security Governance Frameworks in the Cloud Computing Environment. Journal of Universal Computer Science 18(6), 798-815 (2012)
15. Petersen, K., Feldt, R., Mujtaba, S., Mattsson, M.: Systematic mapping studies in software engineering. Proceedings of the 12th International Conference on Evaluation and Assessment in Software Engineering, 71-80 (2008)
16. Cruz Zapata, B., Fernández-Alemán, J., Toval, A. (Accessed 2013) Available at: http://dis.um.es/profesores/aleman/SelectedPapers.xlsx
17. Petersen, K.: Measuring and predicting software productivity: A systematic map and review. Information and Software Technology 53(4), 317-343 (April 2011)
18. Diogo A. B. Fernandes, L.: Security issues in cloud environments: a survey. International Journal of Information Security 13(2), 113-170 (April 2014)
19. N. Gruschka, M.: Attack Surfaces: A Taxonomy for Attacks on Cloud Services. In : IEEE International Conference on Cloud Computing, pp.276-279 (2010)
20. ISO/IEC DIS 27017. Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services. Available at: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43757
21. Carrion Senor, I., Fernandez Aleman, J., Toval, A.: Personal Health Records: New Means to Safely Handle Health Data? Computer 45(11), 27-33 (2012)
22. Carrion Senor, I., Fernandez-Aleman, J.L., Toval, A.: Are Personal Health Records Safe? A Review of Free Web-Accessible Personal Health Record Privacy Policies. Journal of Medical Internet Research 14(4), 161-174 (2012)
23. Fernandez-Aleman, J.L., Carrion Senor, I., Oliver Lozoya, P.: Security and privacy in electronic health records: A systematic literature review. Journal of Biomedical Informatics 46(3), 541-562 (2013)
24. Sanchez-Henarejos, A., Fernandez-Aleman, J.L., Toval, A.: A guide to good practice for information security in the handling of personal health data by health personnel in ambulatory care facilities. Atencion Primaria 46(4), 214-222 (2014)
25. K L Ko, R., Jagadpramana, P., Mowbray, M., Pearson, S., Kirchberg, M., Liang, Q., Lee, B.: TrustCloud: A Framework for Accountability and Trust in Cloud Computing. In : IEEE World Congress on Services, Washington, DC, USA, pp.584-588 (2011)
26. Scarfone, K.: Guide to Security for Full Virtualization Technologies. (2011) Available at http://csrc.nist.gov/publications/nistpubs/800-125/SP800-125-final.pdf.
27. United States: United States Code, Title 44: Public printing and documents, Chapter 35 - Coordination of Federal Information Policy, Subchapter III - Information Security, Section 3541. United States Code, U.S. Government Printing Office, Washington, D.C. (1984)
28. Wieringa, R., Maiden, N., Mead, N., Rolland, C.: Requirements engineering paper classification and evaluation criteria: A proposal and a discussion. Requirements Engineering 11(1), 102-107 (2006)
29. Chandrasekaran, B., Josephson, J., Benjamins, V.: What are ontologies, and why do we need them? IEEE Intelligent 14, 20-26 (January 1999)

30. Cachin, C., Keidar, I., Shraer, A.: Trusting the Cloud. ACM SIGACT News 40(2), 81-86 (2009)
31. Zhang, G., Yang, Y., Chen, J.: A historical probability based noise generation strategy for privacy protection in cloud computing. Journal of Computer and System Sciences 78(5), 1374-1381 (2012)
32. Subashini, S., Kavitha, V.: A Metadata Based Storage Model for Securing Data in Cloud Environment. American Journal of Applied Sciences 9(9), 1407-1414 (2012)
33. Chonka, A., Xiang, Y., Zhou, W., Bonti, A.: Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks. Journal of Network and Computer Applications 34(4), 1097-1107 (July 2011)
34. Zhang, X., Wuwong, N., Li, H., Zhang, X.: Information Security Risk Management Framework for the Cloud Computing Environments. In : Proceedings of the 2010 10th IEEE International Conference on Computer and Information Technology, Washington, DC, USA, pp.1328-1334 (2010)
35. Lin, D., Squicciarini, A.: Data protection models for service provisioning in the cloud. In : Proceedings of the 15th ACM symposium on Access control models and technologies, New York, NY, USA, pp.183-192 (2010)
36. Du, J., Gu, X., Yu, T.: On Verifying Stateful Dataflow Processing Services in Large-Scale Cloud Systems. In : Proceedings of the 17th ACM conference on Computer and communications security, Chicago, pp.672-674 (2010)
37. Jarabek, C., Barrera, D., Aycock, J.: ThinAV: Truly Lightweight Mobile Cloud-based Anti-malware. In : Proceedings of the 28th Annual Computer Security Applications Conference, Orlando, USA, pp.3-7 (2012)
38. Kwon, H., Kim, T., Yu, S., Kim, H.: Self-similarity based lightweight intrusion detection method for cloud computing. In : Proceedings of the Third international conference on Intelligent information and database systems, Berlin, Heidelberg, pp.353-362 (2011)
39. Wang, G., Liu, Q., Wu, J.: Hierarchical attribute-based encryption for fine-grained access control in cloud storage services. In : Proceedings of the 17th ACM conference on Computer and communications security, New York, NY, USA, pp.735-737 (2010)
40. Zhang, L., Li, Q., Shi, Y., Li, L., He, W.: An integrity verification scheme for multiple replicas in clouds. In : Proceedings of the 2012 international conference on Web Information Systems and Mining, Berlin, Heidelberg, pp.264-274 (2012)
41. Hay, B., Nance, K., Bishop, M.: Storm Clouds Rising: Security Challenges for IaaS Cloud Computing. In : Proceedings of the 2011 44th Hawaii International Conference on System Sciences, Washington, DC, USA, pp.1-7 (2011)
42. Mowbray, M., Pearson, S.: A client-based privacy manager for cloud computing. In : Proceedings of the Fourth International ICST Conference on COMmunication System softWAre and middlewaRE, New York, NY, USA, pp.5:1-5:8 (2009)
43. Tancock, D., Pearson, S., Charlesworth, A.: A Privacy Impact Assessment Tool for Cloud Computing. In : Proceedings of the IEEE Second International Conference on Cloud Computing Technology and Science (CloudCom), Washington, DC, USA, pp.667-676 (2010)
44. Campbell, R., Gupta, I., Heath, M., Ko, S., Kozuch, M., Kunze, M., Kwan, T., Lai, K., Lee, H., Lyons, M., Milojicic, D., O'Hallaron, D., Soh, Y.: Open Cirrus cloud computing testbed: federated data centers for open source systems and services research. In : Proceedings of the 2009 conference on Hot topics in cloud computing, Berkeley, CA, USA (2009)
45. Balduzzi, M., Zaddach, J., Balzarotti, D., Kirda, E., Loureiro, S.: A security analysis of amazon's elastic compute cloud service. In : Proceedings of the 27th Annual ACM Symposium on Applied Computing, New York, NY, USA, pp.1427-1434 (2012)

46. Lo, C.-C., Huang, C.-C., Ku, J.: A Cooperative Intrusion Detection System Framework for Cloud Computing Networks. In : Proceedings of the 2010 39th International Conference on Parallel Processing Workshops, Washington, DC, USA, pp.280-284 (2010)
47. Dhage, S., Meshram, B., Rawat, R., Padawe, S., Paingaokar, M., Misra, A.: Intrusion detection system in cloud computing environment. In : Proceedings of the International Conference on Advances in Communication and Computing Technologies, New York, NY, USA, pp.235-239 (2011)
48. Oza, N., Karppinen, K., Savola, R.: User Experience and Security in the Cloud - An Empirical Study in the Finnish Cloud Consortium. In : Proceedings of the 2010 IEEE Second International Conference on Cloud Computing Technology and Science, Washington, DC, USA, pp.621-628 (2010)
49. Ryan, M.: Cloud computing security: The scientific challenge, and a survey of solutions. Journal of Systems and Software 86(9), 2263-2268 (September 2013)
50. J, D., AT, S.: Understanding issues in cloud forensics: two hypothetical case studies. Journal of Network Forensics 3(1), 19-31 (2011)
51. Cearly, D.: Case Studies in Cloud Computing. In: Gartner. (Accessed August 2011) Available at: https://www.gartner.com/doc/1761616/case-studies-cloud-computing
52. Zhang, Q., Cheng, L., Boutaba, R.: Cloud computing: state-of-the-art and research challenges. Journal of Internet Services and Applications 1(1), 7-18 (May 2010)
53. Trier Universität: The DBLP Computer Science Bibliography. (sep 2012) Available at http://dblp.uni-trier.de.
54. Ponemon Institute: Security of Cloud Computing Users 2010, LLC. (May 2010) Available at http://www.ca.com/files/IndustryResearch/security-cloud-computing-users_235659.pdf.
55. Ponemon Institute: Security of Cloud Computing Users 2012, LLC. (March 2013) Available at http://www.ca.com/us/~/media/Files/IndustryAnalystReports/2012-security-of-cloud-computer-users-final1.pdf.
56. Doerr, B.: Cloud Insecurity: Not Enough Tools, Experience or Transparency. (Accessed 2012) Available at: http://www.technewsworld.com/story/74890.html
57. NIST Cloud Computing Security Reference Architecture. Tech. rep., National Institute of Standards and Technology (NIST) (2013) Draft Special Publication 500-299. Available at http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/CloudSecurity/NIST_Security_Reference_Architecture_2013.05.15_v1.0.pdf.
58. Florence: The Politics Of Cloud Computing. (Accessed 2012) Available at: http://www.cloudtweaks.com/2012/05/the-politics-of-cloud-computing/
59. PlanetLab. Available at: http://www.planet-lab.org/
60. EmuLab. Available at: http://www.emulab.net/
61. Cluster Exploratory (CluE). Available at: http://www.nsf.gov/cise/clue/index.jsp
62. Amazon web services. Available at: http://aws.amazon.com
63. Eucalyptus. Available at: http://www.eucalyptus.com/
64. Open Cloud Consortium. Available at: http://opencloudconsortium.org/
65. VINI. Available at: http://www.vini-veritas.net/
66. OneLab. Available at: http://www.onelab.eu/
67. Spring, N., Peterson, L., Bavier, A., Pai, V.: Using PlanetLab for network research: myths, realities, and best practices. ACM Special Interest Group on Operating Systems, Operating Systems Review 40(1), 17-24 (January 2006)
68. Ampatzoglou, A., Charalampidou, S., Stamelos, I.: Research state of the art on GoF design

patterns: A mapping study. Journal of Systems and Software 86(7), 1945-1964 (2013)

69. Elberzhager, F., Münch, J., Ngoc, V.: A systematic mapping study on the combination of static and dynamic quality assurance techniques. Information and Software Technology 54(1), 1-15 (2012)
70. Zhang, H., Babar, M., Tell, P.: Identifying relevant studies in software engineering. Information and Software Technology 53(6), 625-637 (June 2011)
71. Budgen, D., Kitchenham, B. A., Charters, S. M., Turner, M., Brereton, P., Linkman, S. G.: Presenting software engineering results using structured abstracts: a randomised experiment. Empirical Software Engineering 13(4), 435-468 (2008)
72. Easterbrook, S., Singer, J., Storey, M., Damian, D.: Selecting Empirical Methods for Software Engineering Research. In : Proceedings of the twenty-second IEEE/ACM international conference on Automated software engineering, Atlanta, Georgia, USA, pp.574-574 (2007)
73. Rong, C., Nguyen, S., Jaatun, M.: Beyond lightning: A survey on security challenges in cloud computing. Computers & Electrical Engineering 39(1), 47-54 (2013)
74. Seddon, J., Currie, W.: Cloud computing and trans-border health data: Unpacking U.S. and EU healthcare regulation and compliance. Health Policy and Technology 2(4), 229-241 (2013)
75. Subashini, S., Kavitha, V.: A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications 34(1), 1-11 (2011)
76. Lee, T., Kim, H., Rhee, K.-H., Uk, S.: Design and Implementation of E-Discovery as a Service based on Cloud Computing. Computer Science and Information Systems 10(2), Special Issue 703-724 (2013)
77. Stein, S., Ware, J., Laboy, J., Schaffer, H.: Improving K-12 pedagogy via a Cloud designed for education. Journal of Information Management 33(1), 235-241 (February 2013)
78. Alamri, A., Hossain, M., Hassan, M., Hossain, M., Alnuem, M., Ahmed, D., Saddik, A.: A Cloud-Based Pervasive Serious Game Framework to Support Obesity Treatment. Computer Science and Information Systems 10(3), 1229-1246 (2013)
79. Chen, C.-L., Tsaur, W.-J., Chen, Y.-Y., Chang, Y.-C.: A Secure Mobile DRM System Based on Cloud Architecture. Computer Science and Information Systems 11(3), 925-941 (2014)
80. Li, J., Li, B., Wo, T., Hu, C., Huai, J., Liu, L., Lam, K. P.: CyberGuarder: A virtualization security assurance architecture for green cloud computing. Future Generation Computer Systems 28(2), 379-390 (2012)

Belén Cruz Zapata received her Engineer's degree in Computer Science from the University of Murcia in Spain, specializing in software technologies and intelligent and knowledge technologies. She earned an M.Sc in Computer Science and is now working in her Ph.D on the Software Engineering Research Group from the University of Murcia. Her research is focused on mobile technologies in general and also applied to medicine. Belén is currently working as a mobile developer for Android and iOS in the San Francisco Bay Area at Groupon.

José Luis Fernández-Alemán is an Associate Professor at the University of Murcia (Spain), where he is a member of the Software Engineering Research Group. He received his B.Sc. (Hons.) degree in 1994 and his Ph.D. degree in 2002, both in Computer Science from the University of Murcia. He has published more than 20 JCR papers in the areas of requirements engineering and software engineering in the e-health, e-learning and mobile development domains and its application to the fields of computer science, medicine and nursing. Publications include articles in highly ranked international journals such as IEEE Computer, IEEE Software, REJ, IEEE Transactions on Software Engineering, JMIR, JBI and NET.

Ambrosio Toval Álvarez is a full professor at the University of Murcia, in Spain. He holds a BS in Mathematics from the University Complutense of Madrid, and received a Ph.D. in Computer Science (cum laude) from the Technical University of Valencia. He is involved in a variety of applied research and development projects with industry and conducts research and technology transfer in the areas of requirements engineering processes and tools, privacy and security requirements and applications in the e-health, e-learning and mobile development domains. He has published in the same topics in international journals, such as IEEE Software, IST, REJ, Computer Standards & Interfaces, IET, IJIS, etc. Dr. Toval is currently the Head of the Software Engineering Research Group, at the University of Murcia

Received: February 05, 2014; Accepted: October 05, 2014