Cloud Computing Security Requirements and Solutions: a Systematic Literature Review

Patrick Höner
University of Twente
P.O. Box 217, 7500AE Enschede
The Netherlands
p.honer@student.utwente.nl

ABSTRACT
Although the technology and its application are not new, the rising awareness and implementations of cloud services and its underlying technologies cause the need for security requirements being up to date. Cloud computing security requirements have been addressed in publications earlier, but it is still difficult to estimate what kinds of requirements have been researched most, and which are still under-researched. This paper carries out a systematic literature review by identifying cloud computing security requirements from publications between January 2011 and March 2013. It will categorize these requirements in a framework and assess their frequency of research. The paper will then identify changes in the assessment of requirements and proposed solutions compared to publications prior to 2011.

It has been found that the most researched sub-factors of security requirements are: Access Control, Data Integrity and Privacy & Confidentiality. Most under-researched areas are Recovery and Prosecution, with Non-repudiation and Physical Protection closely followed. Various improvements and nested methodologies in current approaches were identified rather than new solutions.

Keywords
Cloud Computing, Security Requirements, SaaS, Software as a Service, Literature Review, Change, Security factors

1. INTRODUCTION
Cloud computing (CC) is an evolving term or paradigm, implying the use of configurable computing resources (hardware, software, network) with its purpose to offer a service to a consumer [53]. By enabling ubiquitous, convenient, on-demand network access [53], its underlying business model contains at least two actors [30]. A cloud provides (1) a cloud service user (CSU) the privilege of access to an application (software), platform or infrastructure "as a service". This term in turn implies that a CSU is making use of a service offered by a (2) cloud service provider (CSP). This said service is usually delivered or transferred by a web browser, mobile app or desktop application on the client side, while the software and its supporting systems are running and data is stored on providers computing machines [53], depending on the service type. By definition of the NIST (National Institute of Standards and Technology), the Cloud Computing model contains three service models. They are referenced to as Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) [53]. Recent publications also identify Network as a Service (NaaS) as an upcoming service type in the vehicle and telecommunication field [47]. Depending on the type of cloud and its deployment model (private, community, public, hybrid [53]), the CSUs are guaranteed either more or less control over the connected computing resources. The degree of control hereby directly relates to security matters, and for all types of cloud services, security has been ranked as the greatest challenge as conducted by a survey of IDC [45]. This causes the need for detailed insights into this field. The main focus of this paper is on public clouds or (public) SaaS security, since they incorporate and cover a great amount of necessary security aspects of the other service levels and deployment models due to hierarchical relations and their implications [19, 53].

The retrieved requirements of the literature review will be assessed in a framework by Firesmith [13] along with their frequency of research and addressed solutions.

In the next sub-sections the problem statement and research questions are formulated. Section 2 describes the research method. Section 3 deals with related work and Section 4 then classifies the papers according to the proposed framework. Section 5 deals with a discussion on the findings, while section 6 elaborates on RQ4. Limitations and validity threats are discussed in Section 7 and conclusions are presented in section 8.

1.1 Problem Statement
Although cloud computing have been researched earlier, the recent increased use of cloud services require up-to-date insights into necessary security requirements and its solutions. It is hard to identify which kinds of requirements have been researched most and which are – still – under-researched.

The objective of this paper is to provide a comprehensive and structured overview of the types of security requirements investigated in the area of in cloud computing and the proposed solutions to deal with these requirements. This paper thus informs fellow researchers on what is known in published empirical studies about security requirements in cloud computing and pinpoints to those types of security requirements that have received much research effort and those that have been under-researched. It moreover addresses and helps consultants and developers with a detailed overview to quickly find and address gaps in cloud security issues.

1.2 Research Questions
This research effort will thus aim to address the following research questions (RQs):

19th Twente Student Conference on IT, June 24th, 2013, Enschede, The Netherlands.

RQ1: What cloud security requirements have been addressed in recent publications (2011-2013)?

RQ2: What solutions are offered to them?

RQ3: Which cloud security requirements have been under-researched?

RQ4: What changes can be identified in addressing cloud security requirements and solutions in the period of 2011-2013 compared to before 2011?

2. METHOD OF RESEARCH

The stated research questions will be answered by carrying out a systematic literature study [26]. The search for literature sources will focus on the usage of Scopus, Web of Science and Google Scholar.

As an initial search string the term "security AND ({software as a service} OR SaaS)" was used. Searches were conducted in Article Title, Abstract and Keywords. It has been observed that the term "cloud" was sometimes being used without reference to the "as-a-service" terminology [6, 54]. Therefore a second search string was constructed, consisting of "security AND cloud" in Article Titles.

The following limitation criteria were used for filtering the addressed results of publications and setting boundaries for this research: (1) limitation of publications by document type of either articles or conference papers (2) limitation by English publications only (3) limitation by publication date between 2011 and now (2013) and (4) the subject area must either include fields of computer science, engineering or business to be relevant for this research's scope.

We would like to point out that the present work is focused on publications in the period of 2011-2013, because empirical publications published before 2011 have already been studied by other researchers [19]. We will use this reference later in our study (namely in Section 6) to compare our findings with the findings of this earlier study and identify the changes that are observed in the period of 2011-2013.

The initial search in Scopus returned a result of 121 valid publications with the mentioned boundaries. As a first indicator of the increased volume of research papers on cloud computing, the result for all valid publications before 2011 amounts to only 93. The results for Web of Science and Google Scholar are estimates, since the mentioned search boundaries are more difficult to set.

The initial result of the literature search with search strings and boundaries is presented in Appendix A. After manual review for relevance of the papers the following refinement criteria for inclusion and exclusion were set:

Inclusion criteria: (1) Cloud security or SaaS security must be the major topic or amongst the major topics of publications and (2) if multiple publications report the same studies, only the most recent one is selected [19].

Exclusion/Limitation criteria: (1) Non-English publications are not considered, (2) keyword restrictions have been set, deviations of keyword set would exceed reviewable results, (3) publications with a specialized context (governmental, medical) were not considered and (4) non-online articles are not included.

These exclusion criteria at the same time define the limitations of this paper's scope. They are required as they set the general scope and limit of this research to be conducted [26].

The manual review of eligible publications resulted in the following amount of papers to be selected and used in the next steps of this research:

Table 1 - Results of literature search

	security AND SaaS	security AND cloud
Scopus	12 - of 121 (10%)	20 - of 399 (5%)
Web of Science	13 - of 126 (10%)	15 - of 489 (3%)
Google Scholar	2 of 81.100	2 of 54.800

Initial literature review revealed that different frameworks have been published to allow addressing and categorization of security requirements [18, 38, 44]. For the purpose of this study, I chose the framework of Firesmith [13]. This choice was motivated because other authors used it [5] and we wanted to compare the findings in this study with theirs, and hence needed to create a common ground for a meaningful comparison so that we answer RQ4. The framework consists of 9 sub-factors defining the hierarchical taxonomy of decomposition of security as a quality requirements factor [13]. The selected literature will be classified among these 9 sub-factors, which will then identify the most investigated and most under-researched areas and build the systematic overview of cloud computing security requirements.

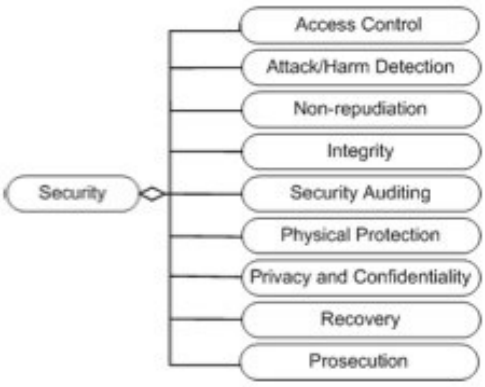

Figure 1 - Taxation of security requirement (Firesmith, 2004)

3. RELATED WORK

In an earlier work, Iankoulova and Daneva [19] already approached a systematic review on cloud security requirements back in Feb, 2011. With this paper, we aim to follow up on their research, taking into account the change on this topic due to aggrandizement in recent years and thus analyze to what extent the focus on requirements has shifted and derived into new issues and challenges in that field.

Additional related work exists, as several researchers have studied the field of cloud computing and its issues and challenges earlier, but an assessment seems to be missing of which requirements are now most researched and which are lacking in efforts of investigation for the mentioned purposes [3, 22, 64].

4. CLASSIFICATION OF LITERATURE BY SECURITY SUB-FACTOR

The selected literature, which includes 57 papers, will now be classified based on the framework proposed by Firesmith [13]. Doing so will enforce identification of areas that are more researched compared to other subjects on a per sub-factor basis. This will provide the basis for answering RQ3 as well as determining suggestions on future work and research. RQ2 will be answered by treating the current state of affairs for the referenced material along with their proposed solutions.

As indicated in Figure 1, the framework of Firesmith from 2004 [13] refers to 9 quality sub-factors:

- Access Control
- Attack/Harm Detection
- Non-repudiation
- Integrity
- Security Auditing
- Physical Protection
- Privacy and Confidentiality
- Recovery
- Prosecution

In the following, each of the 9 sub-factors will be elaborated in detail along with the findings from the corresponding literature sources that belong to each factor. Definitions are derived from Firesmith [13], unless otherwise indicated. Whenever a paper focuses on two or more sub-factors it will be categorized into the category that is most elaborated on. If a paper focuses on multiple requirements it has been categorized as "MULTI" and will be discussed in the corresponding section.

The detailed classification of the literature can be found in Appendix A.

In the following sub-sections, we elaborate on the sub-factors' current state of affairs and proposed solutions.

4.1.1 Access Control

Access control defines the "degree to which the system limits access to its resources only to its authorized externals". Authorized externals can be actual human users, but also services or program fragments, devices or other kinds of systems. Access control may be refined as a combination of Identification, Authentication and Authorization. All three have the common objective to control and supervise a certain range of permissions granted to those users who can claim their identity and be allowed for their defined privileges (e.g. read, modify) over assigned resources. After granting an external permission over a range of resources, access control furthermore has to hold and guarantee this state until a clean and successful termination of the temporary established access takes place [13].

Various frameworks and models have been proposed setting up or defining a collection of standards and procedures to grant the very basic level of protectionism in terms of access control security requirements [7, 20, 56, 65]. They are for example described by the UCON (Usage control) post-obligation model in [65], a framework of combining different security contracts with encryption [7] or one that requires private key exchange along with content encryption [56]. The access control matrix for authorization in clouds is improved by three techniques: data hiding, partial request and data grouping in [20] to improve its main weakness, the amount of time required. The SAML (Security Assertion Markup Language) standard e.g. provides administration and authentication functionality for CSPs [21]. User roles and privileges may then be controlled by standards like XACML (eXtensible Access Control Markup Language) [21].

General current approaches to provide access control range from enforcing authentication through login-credentials, identification of users by (proxy) signatures [4] or requiring private key exchange [66] prior to granting access. Various methodologies of using (symmetric) encryption algorithms for data transmission but also on data storage strengthen these approaches [7, 15, 56, 66]. Both also directly aim to guarantee confidentiality of private data.

An intensively used method of accessing the cloud environment is through a web-browser. This poses a high security concern, because various web-browsers are constantly subject to malicious attacks. Furthermore the transmission of authentication credentials and other data between the CSU and Cloud Service has to be protected during any session. Cryptographic solutions are proposed by using a public key infrastructure, working alongside with SSO (Single-Sign-On) and LDAP [66]. An access control model for CSPs based on semantics is described in [2].

The Lightweight Authentication Protocol (LAP) defined in [58] aims to enhance authentication security. The interoperable security protocol proposed in [46] uses basic standards to define one solution for Cloud and Grid computing. The MADAC model [62] makes use of multi attributes and dynamic access control, while [32] uses a single attribute protection scheme (SAPS).

4.1.2 Attack/Harm Detection

This security sub-factor determines "the degree to which attempted or successful attacks (or their resulting harm) are detected, recorded, and notified".

Solutions for this sub-factor can be differentiated between (1) passive prevention and detection (e.g. using filter mechanisms) and (2) counteractive solutions.

Accessing the cloud with the help of a web-browser poses various security threats as mentioned in the section on access control. Since connections from CSUs to CSPs therefore mainly rely on XML and HTTP protocol transmission, attack/harm detection mechanisms have to start here. XML and HTTP requests are a common subject to vulnerable attacks like (HX)-DoS. Providing a secure mechanism to detect and filter malicious requests is subject to the comber approach of using a filter tree in [24]. Also the ENDER system proposed in [8] aims to detect and mitigate HX-DoS attacks.

The SOTA model [9] (Service-Oriented Traceback Architecture) and its neural network, the Cloud Protector, contain various Cloud TraceBack methods to counter such attack threats. Its authors claim a success rate of 91% in detection and mitigation of HX-DoS attacks. The ENDER system [8] is a follow up on the Cloud Protector mechanisms, named "Pre-Decision, Advance Decision, Learning System" and is described in improving this factor even more. A model of monitoring mechanisms [40] and a real-time network risk

evaluation model [63] are further means for attack/harm detection solutions.

4.1.3 Non-Repudiation

Non-repudiation is defined as "the degree to which a party to an interaction (e.g., message, transaction, transmission of data) is prevented from successfully repudiating (i.e., denying) any aspect of the interaction."

Repudiating interactions (mainly during transmission of data or on their storage) is often counteracted by preventing authorized access in the first place. These techniques are therefore often issued to address access control requirements and are classified as such. Amongst others, they include the exchange of public keys (PKI), certificates or (proxy) signatures.

The SaaS Application Security model for Decentralized Information Flow Control (DIFC, or SAS-DIFC) as proposed in [55], aims to guarantee information security in SaaS applications. Trusted code in this approach controls the dissemination of private data, so that the right user at the right location will receive what belong to him or her. It also offers monitoring mechanisms for user-aware monitoring.

Denying another user from private data that is currently being accessed or transmitted is furthermore an issue of guaranteeing integrity and privacy, which papers connect to non-repudiations in their proposals of solutions [42, 56]. [28] defines the homomorphic distribution verification protocol (classified under "Integrity") enforces non-repudiation implicitly.

4.1.4 Integrity

The integrity sub-factor describes requirements being deployed to protect components of the system from intentional and unauthorized harm or corruption. Integrity requirements can be distinguished for data integrity, hardware integrity, personnel integrity and software integrity. The identified papers almost exclusively focus on data integrity (for example, see [6, 48, 61]). Furthermore (data) integrity was often strongly interconnected to access control requirements.

Frameworks and models were proposed in the literature regarding integrity requirements. A common approach covering requirements in this category is to define Service Level Agreements (SLAs) as contracts between CSU and CSP [61]. Amongst other factors, these SLA define the architecture of the cloud, but also define certain standards. Performing access or transactions on a database e.g. should always follow the ACID principle (atomicity, consistency, isolation and durability) [52]. Other frameworks treat security techniques like cryptographic solutions and dispersed data storage [51]. The principle agent model in [60] is defined to design the auditing strategies that ensure data integrity. Detection and automatic countermeasure are often subject to these models.

Virtualization is a highly important architectural concept of Cloud Computing. This term refers to instantiation of a virtual environment rather than a defined physical machine. Using Virtualization can have severe advantages in terms of scalability, cost-benefits but also security. Virtualization therefore not only enables to isolate faults, viruses or intrusions from other VMs and hardware but can also reduce possible damage of malicious application due to VM isolation [5]. Multi-tenancy is another major important feature in clouds, especially public ones. It provides CSPs, as the name suggests, with more efficient and effective resource utilization by sharing and partitioning mainly services (in SaaS that will lead to specific application service functionalities) among more tenants [54].

Multi-tenancy and virtualization techniques and standards have been addressed in [35]. Other papers deal with a security issues that arises due to multiple VMs being managed on the same host [12]. This causes issues, as one VM might not be safely isolated against malicious or unauthorized access as well as intrusion through another VM running on the same physical host. The principle of the VM fork [12] supports integrity security.

A combined approach of virtualization along with automated monitoring is described in [36]. The monitoring mechanisms constantly checks for vulnerabilities in the cloud architecture, and can immediately report or even take appropriate steps itself and therefore preserves the integrity of data and architecture.

Encryption of data, during storage process or transmission, is also subject for data integrity requirements and is elaborated upon in [6] and [51]. The cryptography hereby is not exclusively limited to software approaches. [48] proposes two cryptographic approaches to data security, hardware and software side.

Another solution is published in [28] and defines the homomorphic distribution verification protocol (HDV) to ensure data security and integrity. The proposed scheme relies on CRS (Cauchy Reed-Solomon) code and token pre-computation. CRS is a so-called cyclic error-correction code, which thus aims to guarantee integrity.

4.1.5 Security Auditing

This sub-factor describes security requirements, in which security personnel are allowed to audit the status, use and vulnerability of security mechanisms by analyzing security-related events.

Security auditing belongs to the dynamic verification approach as distinguished in [41]. In contrast to static approaches it is traditionally achieved by monitoring the execution of systems and checking and verifying its conformity against a set of rules.

In [16] an analysis between existing auditing models has been assessed. Although auditing standards are available, specific cloud-fit auditing standards have not been introduced yet [16]. However, it discusses the applicability of the privacy preserving auditing protocol (also subject to [11]) by the public key based homomorphic linear authenticator (HLA). Moreover it proposes a high performance batch auditing protocol for Third Party Auditors. External Third Party Auditors (TPAs) can be important for CSUs who want their data integrity and security to be assured. This can also be part of the SLA. Last, [11] elaborates on a privacy-preserving TPA protocol that aims to provide private data protection when TPA are involved.

In [37] a logging framework and various guidelines are proposed. Logging is a major help in the assessment of vulnerabilities, faults and access usage. The paper therefore provides a framework for forensics that should eliminate the need for CSUs to "reinvent their own standards".

The solution suite proposed in [41] consists of a (i) three-layered architecture, (ii) new language for expressing monitoring rules and (iii) a finite state machine strategy for improving monitoring engines. A metric driven remote security monitoring approach is described in [49].

4.1.6 Physical Protection

Physical protection indicates the degree to which the system protects itself and its components against physical attacks. 'Physical attack' hereby can refer to natural causes like earthquakes and destruction of infrastructure by natural disasters, but at the same time a malicious intruder stealing physical machines or hardware.

None of the papers focus on physical protection. Natural disasters or theft or similar causes are implied to always be part of SLA between CSUs and CSPs. Even CSPs should be covered for cases like that through insurance terms.

4.1.7 Privacy and Confidentiality

Privacy and confidentiality refers to the degree to which unauthorized parties are prevented from obtaining sensitive information. Many papers are focusing on data security, implying the existence of proper access controls to guarantee confidentiality of private data in the first place. Anonymity towards CSP poses another security requirement measures.

Privacy was often found to be directly connected to access control requirements. Pushing or enforcing strict access control mechanisms relates to a high degree of privacy & confidentiality [21, 52].

Privacy may be split into two kinds of requirements: (1) ensuring confidentiality during access, storage and transmission of data from CSU through the Internet and (2) ensuring confidentiality of CSUs private data from CSP.

The SaaS Confidentiality Risk Management (SCoRiM) framework in [10] proposes a solution to ensure confidentiality of private critical data aimed at small and medium sized enterprises. This can be very important if the CSPs do not provide sufficient conformity for these requirements in their SLAs.

The DOSPA scheme in [31] relies on information dispersal in single tenancy. It enables Data Obfuscation of Single Private Attribute combining geometric transformation and data fragmentation approaches to guarantee data privacy and efficient processing [31].

The user-centric approach for CSUs in [34] uses a client-agent model to overcome privacy barriers. It supports three features: (i) encryption and decryption, (ii) Key management and (iii) filtering techniques. Implementation of this model has to be allowed within SLAs and additionally the CSP has to provide a proper interface.

Another approach to ensure confidentiality is described in [42] by the SaaS Application framework using Information Gateway. The dynamic control mechanism over the executing location enforces a secure data routing. Moreover the framework allows application developers to define their own routing logics. The model also uses techniques of data encryption and data mash up for auditing.

Several other papers focus on privacy and confidentiality, although they might not have been classified as papers that have these two sub-factors as their major topic. [32, 46, 56, 65] are examples of papers focusing on access control, privacy and data integrity to a balanced degree.

4.1.8 Recovery

Firesmith does not provide this sub-factor with a definition, but recovery as a quality sub-factor in terms of Cloud Computing describes the degree to which unintentional manipulated, corrupted or 'lost' (segments of) data may be partially or possibly fully recovered. Recovery itself might be instantaneous, or accessible as an optional functionality for either CSUs or CSPs [13].

It is worthwhile noting that none of the selected literature deals with recovery as a main topic. Nevertheless, with respect to the integrity and security auditing sub-factors, recovery might be realized through hardware or software techniques. Within their SLA, cloud providers usually define contracts for means of data recovery. Thus these kinds of requirements are somewhat implied for cloud providers [51, 61].

While data is physically dispersed on machines through architectural design like virtualization and multi-tenancy, data redundancy and hardware-RAID offers ways to allow for (data) recovery. Roll-back solutions as connected to security auditing models [16] provide software solutions of recovering data.

4.1.9 Prosecution

Similar to the case of the recovery sub-factor, a definition seems to be lacking for Prosecution. Prosecution in terms of Cloud Computing might be twofold: (1) the ability and legislative permission of law enforcement to investigate, seize and prosecute systems subject to breaking the law and (2) the ability to prosecute suspicious or malicious actions and users within the cloud domain. The latter can to some extent be connected to security auditing. As in [11, 16], third party auditing schemes, TPA inclusion by means of SLAs propose solutions to this.

Based on the knowledge of the author who reviews cloud computing magazines regularly, prosecution regarding law enforcement in cloud computing seems to be of flourishing importance in current security discussions in professional circles. Major companies like Microsoft, Apple or Google (all active in the field of cloud computing) got into the focus of revealing private data to (U.S.) governmental bodies (The Guardian, 2013)[1].

However, none of the papers from the literature study revealed to major their topic on prosecution.

4.1.10 Multiple Sub-Factors

An important note on this section refers to the first inclusion (or thus exclusion) criteria in the method of research (see Section 2): "Cloud security or SaaS security must be the major topic or amongst the major topics of publications." Several publications are treating multiple sub-factors in their domain. Therefore one could argue that some of these papers might be too general as they address a broad spectrum of security requirements or factors. However, they did proof to be a valuable information asset for this paper's study of the current state of affairs regarding sub-factors along with available (up-to-date) solutions. Furthermore we are interested in recent developments in the field, as stated in the objective of RQ4.

Papers elaborating on multiple security requirements were thus classified as "MULTI", included in this section and their security proposals will in the following be elaborated upon, not disregarding them in the classification objective.

In Table 2, the Requirements column specifies general requirements being issued by the paper's authors for possible or proposed solutions.

[1] The Guardian, 2013, http://bit.ly/1baaUGj

Table 2 – Papers focusing on multiple security requirements

Ref.	Requirements	Solution
[1]	data violation, network (access threats), integrity & redundancy, isolation, logging, channel protection	best practices, conceptual framework
[5]	security models, security strategies, risk analysis	analysis of security models, issuing of security strategies
[21]	general security, privacy & trust, cryptography	MULTI (for each subject)
[23]	security concerns, protection, multi-tenants, iris, HAIL, global challenge	range of protection mechanisms + auditing framework
[25]	general cloud security; confidentiality, integrity	5 deployment models
[27]	access & identity, trust, privacy, auditing	Security Management as a Service (SMaS) model
[29]	security issues, technical security measures, multiple requirements	5 countermeasure models (current security technologies)
[33]	attack threats, cloud reference model, CRM,	Security Model SM_CRM
[39]	Trusted Platform, User Enabled Collaboration, Security Groups, Data Security, CSU&CSV attestation	4 FPGA based solutions
[52]	survey, security of service delivery models, data risk, current solutions	state of the art security solutions / best practices
[54]	taxonomy for cloud security issues, taxonomy, responsibilities	cloud security architecture model

4.2 Rejected publications in a second round of the review

Throughout the review process, it turned out that seven more papers needed to be excluded from this research's scope due to reasons explained below. First of all, papers that could not be retrieved from any academic database are belatedly excluded due to the non-online exclusion criteria defined in section 2. Second, there were papers in which the abstract was misaligned with the text in the body of the paper. In such cases, during our reading of the abstract, it was our judgment that the paper met our criteria and therefore was to be included. However, while reviewing the text, we found that, for example, the paper either was too general or addressed a topic that only touched security requirements as a side topic. Table 3 presents the references to these seven papers and our reasons for exclusion. Following the guidelines of systematic reviews [26] we considered it important to report on this process and to be explicit about the reasoning we used in making the decisions on paper-exclusion.

Table 3 – Exclusion of seven additional papers at time of review

Ref.	Reason for rejection	Non-online
[14]	Paper addresses the benefits and challenges in three cloud service models, but deems to fail in proposing either functional requirements or (technical) solutions. Furthermore the paper's scope is too general	No
[57]	Paper ranks Key Success Factors in managing information security in cloud computing, no cloud security solutions	No
[17]	Paper focuses on protection of digital media rights in cloud computing by means of a distribution protocol, does therefore not major in cloud security or requirements.	Yes
[43]	Paper focuses on a special case: proposes adaptive security model and policies for business process deployment in cloud, not majoring on cloud security requirements.	Yes
[50]	Paper provides a listing of key challenges and appeals for more research on information security & cloud computing, scope is too general.	Yes
[59]	Abstract unclear about papers scope (security risks on SaaS) and proposed model as solution.	Yes
[66]	Paper addresses CC security issues and mechanisms, but too general, short abstract, and focuses on CSUs only.	Yes

5. DISCUSSION

During the research it has been observed that the in-depth study of the literature and its classification among the different sub-factors took more time than previously assumed and planed. Each paper not only had its own language and style of narration, but the proposed interconnections, terms and proposal of solutions had to be studied in greater detail to gain conclusive insights into terminology, overlaps and approaches.

On the other hand a personal assumption of the author was made that a qualitative and careful classification would be rather the root of a conclusive textual review of the remaining paper.

As indicated in the sub-factor specific sections, it was sometimes not easy to differentiate and classify a paper based on the (major) topic(s) it tackles. As the detailed classification table in the Appendix reveals, for some papers there are two or maybe three options to do so. Not for all papers the distinctive major topic (following the inclusion criteria) could be identified and the paper categorized accordingly. Therefore the following approach was introduced: for every paper posing difficulties in identifying the boundaries and major topic, two or three topics were identified, with one relating to the classified sub-factor and the rest being referred to as "connection". E.g. [15] was identified to be tackling both access control requirements and confidentiality. The paper was thus classified for the first, while a connection-count was noted due to privacy & confidentiality requirements.

This approach aims to slightly balance the strict separation between the security sub-factors. To the current reader it might already be surprising that privacy & confidentiality (along with requirements focusing on 'trust') only amount to 4 out of 50 papers. Taking the connection-factor into account, we found that 10 more papers have an immediate linkage regarding this as equal level of relevancy in their topic's scope.

Table 4 shows the overall distribution of the selected publications classified to the corresponding security sub-factor. Connections refer to the counts of whether this sub-factor was tackled as another (2nd major) topic in already otherwise classified items because of blurred boundaries. Narrow classification details can be reviewed in the Appendix.

Table 4 – Distribution of papers on security sub-factors

Security sub-factor	Amount	Connections	% of total
MULTI	11		22.00%
Access Control	14	5	28.00%
Attack/Harm Detection	5	1	10.00%
Non-repudiation	1	3	2.00%
Integrity	10	6	20.00%
Security Auditing	5	5	10.00%
Physical Protection	0	3	0.00%
Privacy & Confidentiality	4	10	8.00%
Recovery	0	0	0.00%
Prosecution	0	0	0.00%
TOTAL	50	33	100.00%
Exclusions	7		

Table 4 suggests that the most investigated security requirements is Access Control, being the topic of research in nearly 28% of the included publications. The second most studied requirement is Integrity, which is the topic of 20% of the papers in our review.

We also observe that 22% of all papers investigated multiple security requirements. This is not surprising, as dependencies exist among the types of security requirements as described earlier (e.g. [40, 46, 55, 65]).

Overall it was, for example, hard to separate the following correlations (triples) during the classification phase:

- (Access control), data integrity, privacy
- "Data security": mostly referred to as this term, it covers a mixture of (data) integrity and access control, even non-repudiation
- Security auditing, data integrity, privacy
- Attack/harm detection, (physical protection), security auditing

The security sub-factors non-repudiation, physical protection, recovery and prosecution have not been researched in the treated literature, and only minor references and statements about these could be made. One reason for this is that solutions for recovery and non-repudiation might not be researched in connection with cloud computing or the SaaS terminology as a background, but rather general forms of security requirements. Due to our inclusion/exclusion criteria we narrowed down our scope to search for publications in the sectors of computer science, engineering and business. We admit, hardware recovery might be a topic of research posted in field with mathematical engineering background.

The lack of investigation in the prosecution sub-factor might be due to limitation of the literature search by subject area as well. Additionally there seem to be no realistic techniques or possibilities to prevent prosecution from governmental bodies as indicated, although data encryption to provide confidentiality is of major importance.

Furthermore many papers deal with multiple requirements, even when they were devoted to a specific sub-factor. The boundaries of these research efforts sometimes seem blurry due to the overlaps with other sub-factors as mentioned earlier.

Physical protection for example seems to be an under-researched area in security requirements and this might not be surprising. Data integrity and recovery directly relate to this sub-factor. In case of physical theft e.g. data could easily be recovered and restored using information dispersal techniques as described by virtualization, data dispersion and multi-tenancy.

6. COMPARISON TO STATE OF AFFAIRS OF BEFORE 2011

We compared Table 4 in this paper with the respective table about the distribution of publications dated before 2011 as presented in [19]. This comparison led to an initial observation that distribution amongst most investigated and under-research areas in security requirements has not changed noticeably. The scores in [5] and in Table 4 do show similar distribution among the number of papers. It is however noticeable that the approach of considering connections among major and minor topics (defined in this paper) revealed that privacy and confidentiality belong to the three most researched areas.

This study of literature furthermore found that not much 'new' technology has been invented, but rather improved methods or algorithms, nested and cumulative techniques and frameworks are proposed and evaluated. The growing uses of cloud computing solutions require up-to-date security measurement. At the same time main threats seem to be covered by improving current methodologies, like strengthening algorithms, enforcing strict access control and proactive (automated) auditing models. CSUs should consider these in their SLAs and choose a cloud provider that suits their needs.

This study also reveals that techniques to ensure secure access control, guarantee confidentiality of data on storage and transmission, safeguard their integrity along with possibilities for auditing and pro-active countermeasures on attack detections have been profoundly researched since 2011. The application of proposed solutions from general requirements engineering towards the Cloud Computing paradigm has been realized to a great extent too. However, more research in the security sub-factors of non-repudiation and recovery, as well as in prosecution might become important in the next years.

7. LIMITATIONS

With the inclusion of Kitchenhams' "Procedures for performing systematic reviews" [26] we set to cope with the bias of internal validity and professional bias. Correspondence was established with the selection of the included literature and thus the according (re)-definition of inclusion and exclusion criteria. However, this research still faces some limitations that have to be discussed as follows.

First, the research is built on the initial construction of two search strings, which were defined at the beginning of this paper. Although we are interested in explicit security requirements in the field of cloud computing, the tightly related areas of distributed, parallel and grid computing might provide useful information or even concrete correlated security requirements about this research's scope as well. We should recall that the second search string was constructed after manual review revealed that the term "cloud" sometimes was being used without referencing to the "as-a-service" paradigm. The inclusion of three scientific libraries copes with a possible bias of selecting a single academic publications source.

Second, an important threat to the validity of results in systematic reviews is related to the question of whether or not the inclusion/exclusion criteria were consistently applied. In other words, if another researcher reviews the papers' abstracts would he or she decide for inclusion or excluding of the same papers? To make sure the threat of this was limited, the supervisor of the author reviewed independently the abstracts of the 57 papers. The author's and the supervisor's evaluation of the inclusion/exclusion of these papers were compared and differences were found in case of 2 papers. The differences were resolved in a discussion, which enhanced our understanding of the criteria and their application. Moreover, both the author and the supervisor know no author among those of the included papers. This reduces the possibility of injecting professional bias in the selection of the studies, due to friendship or prior collaboration.

Third, we are conscious about the possible bias in classifying the selected publications to the security quality factors in the framework in [6]. As mentioned earlier it was quite difficult to assign a paper to only one sub-factor, because the boundaries among sub-factors were sometimes hard to set. Therefore, another author could classify the same literature depending on the topics it treats differently and thus towards another sub-factor. Overcoming this personal bias seems a bit tricky, because additionally guidelines for the use of Firesmith's framework [13] seem to be missing. Explicit definitions on the usage of a common requirements engineering framework (the basis for Firesmith's framework of the "security" factor) might tackle this dilemma.

8. CONCLUSIONS & FUTURE WORK

This paper reports on a systematic review carried out to answer four research questions. The key findings to these questions are summarized as follows:

RQ1: What cloud security requirements have been addressed in recent publications (2011-2013)?

Our review identified that the following security requirements have been addressed: Attack/Harm Detection, Non-Repudiation, Security Auditing, Privacy & Confidentiality, Access Control and Integrity. The last three requirements are the ones most investigated.

RQ2: What solutions are offered to them?

Solutions to these requirements range from authentication and authorization protocols, the use of Private Key Infrastructure, VM isolation and fork mechanism towards transmission and calculation of encrypted data, but also auditing schemes and countermeasure protection mechanisms. Many of the elaborated and current solutions techniques are not limited to emphasizing rather one security factor, but a range or mixture of sub-factors together.

RQ3: Which cloud security requirements have been under-researched?

The security sub-factors Non-Repudiation, Physical Protection, Recovery and Prosecution define the most under-researched areas in CC security requirements. None of the reviewed papers focused on or had minor overlap with the latter two.

RQ4: What changes can be identified in addressing cloud security requirements and solutions in the period of 2011-2013 compared to before 2011?

Our comparison with a research from 2011 [19] indicated no revolutionary change in the assessment of cloud computing security requirements. In the recent years, not much "new" technology for securing the cloud environment has been introduced, but rather improvements in existing solutions like stronger encryption algorithms, nested authentication credentials or combining approaches are proposed. Attacks needs to be identified and prevented before they can cause any harm and proper (automatic) countermeasure are required to be up to date. We think this accent on improvement indicates an increased maturity of the CC community as researchers might have learned the strong and weak points of the previously proposed solutions in their earlier experiences and are now motivated to leverage this learning to enhance the solutions. This raises new questions for future research. For example, it's interesting to empirically investigate which improvements in a solution work better in what context. Also, we think it is worthwhile understanding the driving forces behind the design of the solutions specific to each security requirement reflected in each sub-factor of Firesmith's framework.

This literature review on cloud computing security requirements and solutions provided a comprehensive overview, which not only targets fellow researchers following up investigating on one or more security sub-factors, but also addresses the interest of consultants or developers: the identified gaps within (under-researched) security requirements make it clear that currently very little useful evidence exists on well-thought out solution designs. Companies therefore might be better off being extremely cautious when implementing vendor's products that claim to solve problems in these under-researched security requirements areas.

9. REFERENCES

[1] Aime, M. D., Lioy, A., Pomi, P. C. and Vallini, M. *Security Plans for SaaS*. Torino, 2011.

[2] Auxilia, M. and Raja, K. *A semantic-based access control for ensuring data security in cloud computing*. Tiruvannamalai,, 2012.

[3] Behl, A. and Behl, K. *Security paradigms for cloud computing*. Phuket, 2012.

[4] Cao, X., Xu, L., Zhang, Y. and Wu, W. *Identity-based proxy signature for cloud service in SaaS*. Bucharest, 2012.

[5] Che, J. H., Duan, Y. M., Zhang, T. and Fan, J. *Study on the security models and strategies of cloud computing*. Tirunelveli,, 2011.

[6] Chen, G., Miao, J., Xie, F. and Mao, H. *A framework for storage security in cloud computing*. Guangzhou, 2013.

[7] Cho, G. H. and Lee, S. A. *A secure service framework for handling security critical data on the public cloud*. Guangzhou, 2012.

[8] Chonka, A. and Abawajy, J. *Detecting and mitigating HX-DoS attacks against cloud web services*. Melbourne, 2012.

[9] Chonka, A., Xiang, Y., Zhou, W. L. and Bonti, A. Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks. *Journal of Network and Computer Applications*, 34, 4 (Jul 2011), 1097-1107.

[10] Chou, Y., Levina, O. and Oetting, J. *Enforcing confidentiality in a SaaS cloud environment*. Belgrade, 2011.

[11] Deshmukh, A. A., Mihovska, A. and Prasad, R. *A cloud computing security schemes:- TGOS and TMS*. Trivandrum, 2012.

[12] Elham, H., Lebbat, A. and Medromi, H. *Enhance security of cloud computing through fork virtual machine*. Agadir, 2012.

[13] Firesmith, D. Specifying reusable security requirements. *Journal of Object Technology*, 3, 1 2004), 61-75.

[14] Gibson, J., Eveleigh, D., Rondeau, R. and Tan, Q. *Benefits and Challenges of Three Cloud Computing Service Models*, 2012.

[15] Gopularam, B. P. and Nalini, N. *Mechanism for secure content publishing for reporting platform hosted on public could infrastructure*. Bangalore, 2013.

[16] Gul, I., Ur Rehman, A. and Islam, M. H. *Cloud computing security auditing*. Gyeongju, 2011.

[17] Guo, Y. J., Zhang, C. G. and Tian, L. Q. Digital media distributing protocol based on cloud computing and proof of security. *Xitong Fangzhen Xuebao / Journal of System Simulation*, 24, 12 2012), 2431-2433+2438.

[18] Haley, C. B., Laney, R., Moffett, J. D. and Nuseibeh, B. Security requirements engineering: A framework for representation and analysis. *IEEE Transactions on Software Engineering*, 34, 1 2008), 133-153.

[19] Iankoulova, I. and Daneva, M. *Cloud computing security requirements: A systematic review*. Valencia, 2012.

[20] Ilanchezhian, J., Varadharassu, V., Ranjeeth, A. and Arun, K. *To improve the current security model and efficiency in cloud computing using access control matrix*. Tamilnadu, 2012.

[21] Jansen, W. A. *Cloud Hooks: Security and Privacy Issues in Cloud Computing*. Koloa, Kauai, 2011.

[22] Jia, W. and Sun, S. *Research on the security issues of cloud computing*. Wuhan, 2013.

[23] Juels, A. and Oprea, A. New approaches to security and availability for cloud data. *Communications of the ACM*, 56, 2 2013), 64-73.

[24] Karnwal, T., Thandapanii, S. and Gnanasekaran, A. *A filter tree approach to protect cloud computing against XML DDoS and HTTP DDoS attack*. Chemnai, 2013.

[25] Kaur, P. J. and Kaushal, S. *Security Concerns in Cloud Computing*. Chandigarh, 2011.

[26] Kitchenham, B. Procedures for performing systematic reviews. *Keele, UK, Keele University*, 332004), 2004.

[27] Krishnan, D. and Chatterjee, M. *Cloud security management suite - Security as a service*. Trivandrum, 2012.

[28] Kumar, P. S. and Subramanian, R. Homomorpic Distributed Verification Protocol for Ensuring Data Storage Security in Cloud Computing. *Information-an International Interdisciplinary Journal*, 14, 10 (Oct 2011), 3465-3476.

[29] Lee, H., Kim, J., Lee, Y. and Won, D. *Security Issues and Threats According to the Attribute of Cloud Computing*. Jeju Island, 2012.

[30] Leimeister, S., Böhm, M., Riedl, C. and Krcmar, H. *The business perspective of cloud computing: Actors, roles, and value networks*. Pretoria, 2010.

[31] Li, L., Li, Q. Z., Shi, Y. L. and Zhang, K. *A New Privacy-Preserving Scheme DOSPA for SaaS*. Taiyuan, 2011.

[32] Li, L., Li, Q. Z., Shi, Y. L. and Zhang, K. SAPS: A Single Attribute Protection Scheme for SaaS. *Information-an International Interdisciplinary Journal*, 15, 1 (Jan 2012), 275-282.

[33] Li, X. L., Chen, J. H., Luo, M. and Ieee *A Simple Security Model based on Cloud Reference Model*, 2011.

[34] Lijo, V. P. and Kalady, S. *Cloud Computing Privacy Issues and User-Centric Solution*. Bangalore, 2011.

[35] Loganayagi, B. and Sujatha, S. *Improving Cloud Security through Virtualization*. Tirunelveli, 2011.

[36] Loganayagi, B. and Sujatha, S. *Enhanced cloud security by combining virtualization and policy monitoring techniques*. Coimbatore, 2012.

[37] Marty, R. *Cloud application logging for forensics*. TaiChung, 2011.

[38] Mellado, D., Blanco, C., Sánchez, L. E. and Fernández-Medina, E. A systematic review of security requirements engineering. *Computer Standards and Interfaces*, 32, 4 2010), 153-165.

[39] Mondol, J. A. M. and Ieee *Cloud Security Solutions using FPGA*, 2011.

[40] Monfared, A. T. and Jaatun, M. G. *Monitoring intrusions and security breaches in highly distributed cloud environments*. Athens, 2011.

[41] Munoz, A., Gonzalez, J. and Mana, A. A Performance-Oriented Monitoring System for Security Properties in Cloud Computing Applications. *Computer Journal*, 55, 8 (Aug 2012), 979-994.

[42] Nishikawa, K., Oki, K. and Matsuo, A. *SaaS application framework using information gateway enabling cloud service with data confidentiality*. Hong Kong, 2012.

[43] Ouedraogo, W. F., Biennier, F. and Ghodous, P. *Adaptive security policy model to deploy business process in cloud infrastructure*. Porto, 2012.

[44] Pfleeger, S. L. A framework for security requirements. *Computers and Security*, 10, 6 1991), 515-523.

[45] Popović, K. and Hocenski, Z. *Cloud computing security issues and challenges*. Opatija, 2010.

[46] Rajagopal, R. and Chitra, M. *Trust based interoperability security protocol for grid and Cloud computing*. Coimbatore, 2012.

[47] Rangarajan, S., Verma, M., Kannan, A., Sharma, A. and Schoen, I. V2C: a secure vehicle to cloud framework for virtualized and on-demand service provisioning. In *Proceedings of the Proceedings of the International Conference on Advances in Computing, Communications and Informatics* (Chennai, India, 2012). ACM.

[48] Rohini, T. *Comparative Approach to Cloud Security Models*. Mumbai, 2011.

[49] Savola, R. M. and Ahola, J. *Towards remote security monitoring in cloud services utilizing security metrics*. Tbilisi, 2012.

[50] Sehgal, N. K., Sohoni, S., Xiong, Y., Fritz, D., Mulia, W. and Acken, J. M. A Cross Section of the Issues and Research Activities Related to Both Information Security and Cloud Computing. *Iete Technical Review*, 28, 4 (Jul-Aug 2011), 279-291.

[51] Sood, S. K. A combined approach to ensure data security in cloud computing. *Journal of Network and Computer Applications*, 35, 6 (Nov 2012), 1831-1838.

[52] Subashini, S. and Kavitha, V. A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, 34, 1 2011), 1-11.

[53] Technology, N. I. o. S. a. *The NIST Definition of Cloud Computing*. U.S. Department of Commerce,Gaithersburg, 2011.

[54] Tianfield, H. *Security issues in cloud computing*. Seoul, 2012.

[55] Tingting, L. and Yong, Z. *A Decentralized Information Flow model for SaaS application security*. Hong Kong, 2013.

[56] Tran, D. H., Nguyen, H. L., Zha, W. and Ng, W. K. *Towards security in sharing data on cloud-based social networks*. Singapore, 2011.

[57] Wang, J. S., Liu, C. H., Lin, G. T. R. and Ieee *How to Manage Information Security in Cloud Computing*. Anchorage, 2011.

[58] Wang, S. C., Liao, W. P., Yan, K. Q., Wang, S. S. and Tsai, S. H. *Security of cloud computing lightweight authentication protocol*. Kaohsiung, 2013.

[59] Wang, Y. C. and Chen, S. *Analysis of Informatization Construction for SMEs with SaaS model*. Shenzhen, 2011.

[60] Xiao, M. and Chen, L. Integrity auditing strategy design for data storage security in cloud computing. *Journal of Computational Information Systems*, 8, 23 2012), 9779-9789.

[61] Xiao, Z., Hong-tao, D., Jian-quan, C., Yi, L. and Lei-jie, Z. *Ensure Data Security in Cloud Storage*. Guanxi, 2011.

[62] Yan, D., Yang, F. and Tet, Y. Servies security architecture and access control model for cloud computing. *China Communications*, 8, 6 2011), 44-50.

[63] Yang, J., Wang, C., Liu, C. and Yu, L. Cloud computing for network security intrusion detection system. *Journal of Networks*, 8, 1 2013), 140-147.

[64] Zhang, Y. and Zhang, Y. *Cloud computing and cloud security challenges*. Hokkaido, 2012.

[65] Zhu, J. and Wen, Q. *SaaS access control research based on UCON*. Guangzhou, 2012.

[66] Zissis, D. and Lekkas, D. Addressing cloud computing security issues. *Future Generation Computer Systems-the International Journal of Grid Computing and Escience*, 28, 3 (Mar 2012), 583-592.

APPENDIX

A. CLASSIFICATION OF LITERATURE

Interested readers are welcome to review the detailed classification of literature here:

https://docs.google.com/file/d/0B1kCzpzBWEmDNHpLUDNWX05aeFE/edit?usp=sharing

http://bit.ly/18px2QV