Ouedraogo et al. Journal of Cloud Computing: Advances, Systems and Applications (2015) 4:12
DOI 10.1186/s13677-015-0037-5

Journal of Cloud Computing
a SpringerOpen Journal

REVIEW Open Access

Security transparency: the next frontier for security research in the cloud

Moussa Ouedraogo[1*], Severine Mignon[1], Herve Cholez[1], Steven Furnell[2] and Eric Dubois[1]

Abstract

The recent advances in networking and the ubiquity of the Internet have enabled the emergence of cloud computing as a viable solution for a convenient, elastic and economical usage of services. In spite of these apparent advantages, the cloud model presents some challenges that hamper its wider adoption, most of which relate to security and privacy. This paper provides a review of the current initiatives devised by both academia and industry for addressing the security concerns inherent to the cloud model. Our analysis of the state of the art reveals that although initiatives such as SLA and virtual machines monitoring, and recent development in encryption mechanisms, have contributed to addressing some of the salient issues of security and privacy in the cloud, larger initiatives, other than standards, aiming at enabling security transparency and a mutual auditability in the cloud remain to be seen. With this in mind, the paper proposes some routes towards related solutions by discussing a number of desiderata for establishing a better security transparency between a Cloud Service Provider (CSP) and a Cloud Service Consumer (CSC). Given the current reluctance of some major businesses to embrace the trend, owing mainly to the devolution of some of the security aspects to a third party, the authors argue that undertaking some initiatives in that direction is a key to sustaining the current momentum of the cloud.

Keywords: Security and protection; Cloud Services; Security transparency; Mutual audits; Trusted cloud services

Introduction

It has been acknowledged that the current advances in virtualisation and the ubiquity and pervasiveness of high-speed networking are driving a complete rethink of the paradigm whereby organisations deploy and manage their own services and infrastructures [1]. This has mainly resulted in the increased popularity of service provisioning models such as cloud services. Beside the technological context that has made it possible, there is an economical and performance incentive for embracing the trend. Indeed, the complexity of today's systems and networks, and the cost associated with their management and maintenance, has prompted the re-emergence of the old type computing usage characterised by timesharing, usage-based pricing and shared resources [2]. The timesharing model arose because computers were expensive and hard to maintain, while in contrast, modern computers and networks are drastically cheaper, but still hard to maintain. Once again, it becomes convenient and cheaper to outsource, especially when one considers that computing is now seen as a utility. Despite these benefits, security in cloud services poses increased challenges for consumers, since both the data and programs of the consumers may reside in geographically different locations, yet often within the Cloud Service Providers' (CSPs) premises. Several studies (including [3–5]) have pointed out that despite the potential benefits of cloud services, security remains one of the major concerns that hinders a large scale adoption by big and medium-size corporations. In fact, having one's data stored and processed within one's organisational administrative domain gives the chance to select the appropriate protection mechanisms, and decide who may or may not have access to the data. Once the processing and/or storage of the data is delegated to a third party, one can only hope that the decisions on security matters will be as good as one would expect. This has led numerous surveys and technical contributions to focus on the security of cloud-based services. For instance, Subashini and Kavitha [6] surveyed the security concerns pertaining to each of the cloud models (Software as a Service-SaaS, Platform as a Service-PaaS and Infrastructure as a Service- IaaS) with a synopsis on the existing security solutions. According to

* Correspondence: moussa.ouedraogo@list.lu
[1]Luxembourg Institute of Science and Technology, Esch/Alzette L-4362, Luxembourg
Full list of author information is available at the end of the article

the authors, the main concern with SaaS, as reported by enterprise actors, is the lack of visibility about the way their data is stored and secured. In addition, they are concerned about insider breaches, along with vulnerabilities in the applications and systems' availability that could lead to loss of sensitive data and money. With respect to IaaS, the authors highlighted it only provides basic security such as perimeter firewall and load balancing. Thus applications moving into the cloud will need higher levels of security provided at host level. The PaaS model is said to be prone to serve as a cover environment for hackers, as one can easily leverage the PaaS cloud infrastructure for malware command and control and target IaaS applications [6]. Indeed, the capability of PaaS cloud to provide an environment for full life cycle software development and testing hides a darker side or so called "Malware as a Service". The key concern is that hackers, rather than running their malicious code from local resources, will now tend to leverage the PaaS to develop and manage malicious codes that would ultimately take aim at resources available on the Internet included IaaS infrastructure.

Lombardi and Di Pietro [7] followed in a similar path by first investigating the security issues pertaining to the cloud models before elucidating the key requirements for a protection system. Their contribution, referred to as Advanced Cloud Protection System (ACPS), is based on security extensions of the Linux Kernel Virtual Machine. The ACPS purports to actively protect the integrity of the guest Virtual Machines (VMs) and the distributed computing middleware, against intruders and malware, by allowing the host to monitor guest virtual machines and infrastructure components [7].

In a similar way, the security in multi-tenant software platforms, resulting from the PaaS model, has been the object of the analysis conducted by the survey of Rodero-Merino et al. [8]. Here the authors explored the technical vulnerabilities within the underlying platform that support multi-tenancy in the PaaS model, namely container systems such as Java and .NET. The authors noted that isolation of codes from different Cloud Service Consumers (CSCs) within a PaaS was necessary to limit the impact of a faulty code on other adjacent applications. In fact, as noted earlier, the code executed by the PaaS system may be untrusted, either because they are malware code developed and/or running on the PaaS, or because best practices on safe coding were not followed leading to vulnerabilities that could be exploited. As a result it is imperative for the CSP of a PaaS to identify and implement the necessary mechanisms that can enforce security policies aiming to decrease the risks involved in running such code.

The comprehensive work by Vaquero et al. [9] has been devoted to the examination of the security threats relating the IaaS model, in particular those induced by the virtualisation and multi-tenancy aspects of the cloud. From the initial stages of a VM life cycle (definition of the OS) via the creation and customisation of the VM, to its transportation to the hypervisor, storage, deployment and runtime, the authors proceeded to mapping each step of the VM's life cycle to known threats, namely those identified by the Cloud Security Alliance (CSA), along with existing solutions as can be seen in Table 1. The authors subsequently concluded that access control and encryption mechanisms were the techniques relied upon for dealing with security concerns resulting from virtualisation. The aforementioned threats are further described in Section 2.

To all the above, we can add the extensive body of work on security of cloud services that has largely focused upon debating the peculiarities of security in cloud services (example of [10–12]), and describing the security challenges and some solutions associated to the model [11–19]. What has been missing so far, especially with respect to the surveys conducted, is an analysis of how known security concerns along with their existing solutions contribute respectively, in exacerbating or improving the mutual trust between the CSP and CSC. This is not to overlook the colossal security challenges that come with the cloud. Instead, we argue that for the model to gain in momentum, it is imperative to dedicate some research on the security transparency and help boost the confidence of its users on a critical security matters that may be devolved to a third party.

The contribution of this paper is two-fold: First we explore the security initiatives currently tailored for enhancing the trust relationship in the cloud environment. This paper provides a review of such initiatives emanating from both academia and industry. Secondly, the paper discusses how such initiatives have had limited success in appropriately addressing the salient need for security transparency between the two main stakeholders i.e. the CSP and the CSC, before describing a number of desiderata that may

Table 1 Mapping of VM's life cycle threats and security solution [9]

Threats	VM Life cycle stage	Security solutions
NA	Image definition	NA
NA	Image Creation	NA
NA	Image Customisation	NA
Threats 4and 5	Transportation	Cryptographic protection
Threats 1–5	Storage	Cryptographic protection
Threats 1, 2, 3 and 5	Deployment	Encrypted boot and data partition Custom binding
Threats 1-6	Contextualisation	Custom binding
Threats 1, 3,4,5,6 and 7	Runtime	Deviation from "normal"
Threats 2, 3 and 5	Undeployment	VM introspection (VM memory consistency checks

be carried out by researchers and the industry for promoting and establishing a trusted cloud environment.

The paper is organised as follows: Section II provides background information on cloud security concerns. Section III reviews some trusted cloud computing platforms and VM monitoring methods. Section IV is devoted to the review of efforts aiming at establishing security transparency through the definition and monitoring of a Service Level Agreement (SLA). In Section V, we analyse the role of governance in making the cloud more security trustworthy. Section VI analyses the current efforts in data encryption and their potential to make the cloud more trustworthy. In Section VII, we discuss how the aforementioned initiatives fare in delivering security transparency in the cloud, before laying down a number of desiderata that may be considered for strengthening such a transparency. Section VIII concludes the paper and discusses our future work.

Security and privacy concerns in cloud services

Security-related issues within the cloud differ little from traditional IT solutions, since cloud computing itself is a result of combining existing computing techniques, such as virtualisation, grid computing, and service-oriented computing. According to Chen et al. [10], few cloud computing security issues are fundamentally new or fundamentally intractable, as many of the problems often cited (such as downtime, data loss, and password weaknesses) already received attention dating back to the time-sharing era. Nonetheless, the authors stressed that two facets are to some degree new and fundamental to cloud computing: the complexity of multi-party trust considerations, and the subsequent need for mutual auditability. Both aspects have, to some extent, have contributed to exacerbating the perception of insecurity in the cloud realm.

Indeed, in the cloud, the data and the mechanisms necessary for its processing may reside in the CSP's premises. This makes security within the cloud stringently dependent on the provider's security; prompting the argument that "*cloud computing is about gracefully losing control while maintaining accountability*" [20, 21]. The stored information may be subject to the legislation of the country where it is stored physically. As the data processing of cloud services can be carried out in geographical locations that are not even necessarily known by the CSCs, security and privacy management is challenging. Some privacy legislation requires that the critical data should reside only in a specific country, addressed by the legislation. In general, the privacy threats to the CSC's information can be different depending on the privacy terms of the service. In addition to ensuring the privacy of the stored and/or processed information, any information generated and stored regarding the actual transaction itself may need to be confidential.

The security responsibilities of both the CSP and the CSC will basically depend upon the cloud service model. In the case of SaaS, the service security and the liability expectations of the service provider are contractually specified in a formal document. In the case of PaaS or IaaS, it is the responsibility of the consumer's system administrators to securely manage the service, while some of the security responsibilities (namely those relating the security of the underlying platform and infrastructure) are liable to the provider.

The deployment model of a cloud service affects the choice of security mechanisms. Indeed, the security needs are expected to increase in scale as one moves from a private to a public cloud setting. This is mainly because the context of a private cloud differs very little from a traditional information system, especially if the private cloud is managed by the very same company that uses the service. In contrast, the hybrid and public cloud models increase such security concerns, as the models expose the CSC's information to a pool of individuals either sharing the same resources or external to the cloud. In the hybrid and public cloud, special attention should be paid to the confidentiality of the transactional information, in addition to the storage and processing of the consumer's information. In fact, either maliciously or accidentally, cloud provider's employees can tamper with or leak a company's data; an action that can severely damage the reputation or finances of a company [22]. Other security concerns that have been thoroughly discussed in the literature include those related to the multi-tenancy aspect of cloud services, reliability and availability. The multi-tenancy concerns relate to attacks from other consumers, who may be competitors or simply hackers, co-located on the same infrastructure, such as servers, hard disks, virtual machines. Similarly, the reliability and availability of cloud services are dependent on those of the Internet, since access to those services is made through an Internet connection. Thus, downtimes of such services can occur even in the case of large-scale providers such as Amazon and Rackspace [23].

Another way of looking into the security concerns in the cloud model is through the analysis of the threats it faces. A commonly referenced list of threats for cloud is that of the CSA [16], as depicted in Table 2. It is important to note that a revised list of threats is provided by the CSA [24]. However such a list remains a mere rebranding of some of the threats (for instance *threat 5* is split into two threats *Data breach and Data loss;* and *threat 7* known as *unknown security profile* is renamed *Insufficient due diligence*) while the few added threats can be seen as obvious consequences of the lists proposed in the previous CSA document [16] (for example, the newly added threat of *Denial of service* for the cloud is a result of *Shared technology issue* whereby a lax in

Table 2 Overview of cloud related threats as defined by the Cloud Security Alliance [16, 24]

CSA defined tsreats	Description
Threat 1: Abuse and nefarious use of cloud computing	Malicious code authors, spammers and other criminals can abuse the relative anonymity behind some of current cloud services.
Threat 2: Insecure interfaces and APIs	A set of software interfaces are utilized by the CSPs for CSC interaction of the services. The security and availabilty of cloud services depends upon the security of the basic interfaces, such as Application Programming Interfaces (APIs).
Threat 3: Malicious insiders	The threat of malicious insider is amplified for cloud services due to the convergence of Information Technology (IT) services and customers under a single management domain.
Threat 4: Shared technology issues	CSPs deliver services in a scalable way. Some underlying component parts of the cloud infrastructure were not originally designed for that environment, and can potentially cause security problems. The main concern is that a single vulnerability or misconfiguration can lead to a compromise across an entire provider's cloud
Threat 5:Data loss or leakage	The threat of data compromise increases in the cloud, due to the number of interactions between risks and challenges which are either unique to cloud, or more dangerous because of the architectural or operational characteristics of the cloud environment.
Threat 6: Account or service hijacking	Phishing, fraud and exploitation of software vulnerabilities can be used for account or even service hijacking.
Threat 7: Unknown Security Profile	The reduction of cost of ownership induced by the cloud also resulted in more complex analysis of a company's security posture. More tenants imply increased complexity in detecting who is using the infrastructure and how this is done.

security may lead to a broader security issues for the overall cloud service infrastructure, with impact on several CSCs. Consequently, the threats hereafter reviewed will be principally based on the previous version which is complete enough to comprehend the core security issues related to cloud based services. As we aim to explore the angle of security transparency between the CSP and the CSC, it is relevant to analyse each of those threats in view of identifying those contributing one way or the other to the fear of the CSC to embrace the cloud. Only after this, one could elaborate on the set of actions undertaken both by academia and industry towards reducing, if not eliminate those concerns.

Threat 1 (*Abuse and nefarious use of cloud computing*), is one that has been gaining in proportion recently. Indeed, there is now evidence that botnets are operating within the cloud, as criminals try to amplify the magnitude of their attack by leveraging the technology offer by the cloud, while remaining undetectable at the victim's computer [25]. This is well exemplified by the "Amazon Zeus botnet" incident involving Amazon EC2's infrastructure [26], whereby cybercriminals, by initially hacking into a service hosted by the Amazon cloud infrastructure, were able to install command-and-control infrastructure with the aim of infecting client computers and stealing their banking credentials. Importantly this threat is of great concern for companies or individuals within or outside of the cloud, given that the computation powers or amenities of the cloud could be leveraged for targets beyond the CSP's infrastructure.

Threat 2 (*Insecure interfaces and APIs*): Application Programming Interfaces (APIs) provide a thorough mapping of software or a service. The benefit of publicising APIs by the CSP is two-fold [27]:

1. To expose the available features of cloud components to their customers
2. To enable customer(s) to formulate their deployment re-architected, if needed, for better mutual benefits.

The downside is that this also forms a body of useful information on the actual features and architecture of the service, which may be exploited for a malicious purpose, especially when harbouring some technical flaws. It is therefore imperative that CSPs strictly limit the information displayed on the functionalities of their service through usage of such technique as encryption, abstraction and encapsulation.

Threats 3–5 relate to the issues of *data security in the cloud*, namely its Confidentiality, Integrity and Availability (CIA). Such threats may be due to malicious insider actions (unscrupulous cloud employees or an ill-intentioned tenants co-located on the same physical resource); or owing to the CSC being unable to obtain his data as a result of a termination of the CSP activities. These threats have been at the forefront of reasons behind the slow and cautious move of companies toward the cloud. The good news, however, is that researchers from both academia and industry are starting to devise solutions, including new encryption methods, for ensuring data confidentiality and integrity security. We expand on this later in Section 6.

Threat 6 (*Account or service hijacking*) relates to the fact that the security of the cloud service is only as good as at its weakest link. For instance, a vulnerability at a tenant

application may result in the jeopardy of the whole service, as witnessed by the Amazon Zeus botnet incident. Although such a threat can be very cumbersome to contain (as it depends on many factors and actors of the cloud), actions such as user education about security and VM monitoring are often relevant safeguards.

Threat 7 (*Unknown Security Profile*) relates to the difficulty to determine ones' security posture in the cloud context, given that its security level depends on multiple players including the concerned CSC; the CSP or chain of CSPs which is not always known to the CSC; and Other CSCs. To help the CSC keep an eye on the service security and performance, and have some sort of confidence on the actual service utilised, Service Level Agreement (SLA) and monitoring, and security audits are often performed. We further elaborate this aspect in Section IV.

Table 3 provides a summary of the most common security solutions adopted against the threats that impact on the adoption of the cloud model.

In the following sections, we discuss the initiatives that are being devised towards fostering more security transparency between the level of visibility into security policy and operations offered by the CSP to the CSC [28]. Those set of initiatives conducive to enhancing the trust relationship in the cloud environment have come mainly in the form of virtual machines monitoring; usage of encryption; certification, audits and monitoring of Service Level Agreement (SLA).

The usage of trusted cloud computing platforms and monitoring of virtual machines

Besides the debate on whether the cloud service is worth the hype surrounding it, some initiatives focusing on the usage of a trusted platform and the monitoring of Virtual Machines, have emerged as potential solutions for addressing the issue of security and privacy in the cloud.

Santos et al. [22] proposed the Trusted Cloud Computing Platform (TCCP), which aims to ensure the confidentiality and integrity of the data and computation undertaken by the provider. Using a program associated to TCCP, a customer may be able to detect whether the data or computation has been tampered with or been accessed even by the provider. Subsequently, the customer may decide on whether to terminate a VM should they notice any abnormality. In particular, the TCCP needs to guarantee that the VM is launched on a trusted node and that the system administrator is unable to inspect or tamper with the initial VM state as it traverses the path between the user and the node hosting it. The TCCP approach builds upon a traditional trusted platform, such as TERRA [29], to ensure the integrity and confidentiality in the context of multiple hosts.

Another initiative that uses the concept of trusted platform is the Private Virtual Infrastructure (PVI) proposed by Krautheim [30]. This has suggested a means to allow monitoring in the cloud by combining the trusted platform module (TPM) and a Locator Bot that pre-measures the cloud for security properties, securely provisions the datacentre in the cloud, and provides situational awareness through continuous monitoring of the cloud security. In this approach, security appears as a shared responsibility between the provider and the consumer. Thus, the SLA between the client and the provider is critical to defining the roles and responsibilities of all parties involved in using and providing the cloud service.

The authors in [31] argued that the dependability of cloud services may be attained through the quantification of security for intensive compute workload clouds to facilitate provision of assurance for quality of service. They subsequently defined seven security requirements which include: Workload state integrity, Guest OS Integrity, zombie protection, Denial of Service attacks, malicious resource exhaustion, platform attacks and backdoor protection. Unfortunately the paper does not provide any evidence of effort towards quantification of security as it claimed. Moreover it remains unclear as to how information relating those security requirements may be conveyed to the provider and consumer alike.

De Chaves et al. proposed an initiative to private cloud management and monitoring called PCMONS [32]. The authors argued that despite the peculiarity of cloud services compared to traditional legacy systems, existing tools

Table 3 Cloud security threats and some related solutions based on our survey and the CSA documents [16, 24]

Threats affecting the wider adoption of the cloud	Some related security solutions
Threat 1	Customer CSC's network traffic introspection VM monitoring,
Threat 2	Security Analysis of API Encryption, Access Control encapsulation, abstraction
Threat 3	Supply chain audit including human resource hiring procedure, Security certification, Audits, Use of Trusted Cloud Computing Platform (TCCP)
Threat 4	VM monitoring and cloud audit, Access control, SLA enforcement for patching and vulnerability remediation
Threat 5	API, Access control, Encryption and key management, Use of Trusted Cloud Computing Platform (TCCP)
Threat 6	VM monitoring, Use of Trusted Cloud Computing Platform (TCCP), Access control and authentication
Threat 7	Security certification, Audits, SLA monitoring

and methods for managing networks and distributed systems can be reused in cloud computing management. PCMONS is based on a centralised architecture with the following features [32]: (a) a Node Information Gatherer, which is responsible for gathering local information on a cloud node; (b) Cluster Data Integrator, an agent that gathers and prepares the data for the next layer (the monitoring data integrator); (c) a Monitoring Data Integrator that gathers and stores cloud data in the database for historical purposes, and provides such data to the Configuration Generator; (d) a Virtual Machine (VM) Monitor that sends useful data from the VM to the monitoring system; (e) a Configuration Generator for retrieving information from the database; (f) a monitoring Tool Server that receives monitoring data from different resources (e.g., the VM Monitor); and finally (g) a database where the data needed by the Configuration Generator and the Monitoring Data Integrator are stored. Given PCMONS was developed to respond to the needs of management in private cloud, the need of establishing mutual trust between the provider and the consumer does not arise. Nonetheless, based on our experience in working with similar systems, the proposed architecture may present some interesting features that could easily be expanded to deliver mutual auditability and security transparency and mutual auditability. One way of achieving this would be to consider the monitoring data integrators consoles as part independent service whereby CSCs can, upon the formal specification of their requirements be provided with relevant information on the security of the service they are using.

Overall, it can be said that the research community has moved from debating whether the cloud is a mere hype to devising some tangible initiatives for resolving security issues. Unfortunately the current efforts on trusted cloud computing platforms and monitoring of Virtual Machines have mainly been driven by the need to foster a better management of security for the CSP provider rather than addressing the complexities of multi-party trust considerations (particularly those related to security), and the ensuing need for mutual auditability. In fact monitoring of VMs is meant to be conducted by and for the CSP.

Security transparency through SLA management

According to the interview study conducted in [33], security transparency is emphasized as the main security need in the cloud by security experts. For Rak et al., the mutual trust between a provider and a customer should be considered only in context of an SLA management [34]. Using a cloud-oriented API derived from the mOSAIC project (http://www.mosaic-project.eu/), the authors built up an SLA-oriented cloud application that enables the management of security features related to user authentication and authorization of an IaaS Cloud Provider. This gives the opportunity for the customer to select from amongst a number of security requirements templates, the one that may be appropriate for the nature of his/her application before the provider can set up the configuration of the concerned node accordingly. As noted by the authors, the consideration of SLA in the management of the cloud security provides the consumer with formal documentation about what he/she will effectively obtain from the service. Meanwhile, from the provider point of view, SLAs are a way to have a clear and formal definition of the requirements that the application must respect. However, the initiative by Rak et al. [34], does not go far enough to incorporate means for monitoring and reporting on the fulfilment of such SLA to the consumer. An extension of the work of Rak et al. [35] in the context of the EU FP7 project Specs (http://specs-project.eu/) considered the provision of a platform for providing a security services based on SLA management.

The SLA@SOI project [36] also followed in the path of SLA management in service oriented architectures, which includes cloud technology. The monitoring of SLAs expressed in the SLA specification language of SLA@SOI requires the translation of these SLAs into operational monitoring specifications (i.e., specifications that can be checked by a low level monitor plugged into the SLA@SOI framework). The SLA monitoring in SLA@SOI relies on EVEREST+ [37], which is a general-purpose engine for monitoring the behavioural and quality properties of distributed systems based on events captured from them during the operation of these systems at runtime. The properties that can be monitored by EVEREST are expressed in a language based on Event Calculus [38], called *EC-Assertion*. Similarly, Chazalet discusses SLA compliance checking in cloud environments and uses JMX (Java Management Extensions) technology in the prototype implementation [39]. Their checking approach allows separating concerns related to the probes, information collection and monitoring and contract compliance checking.

The negotiation of SLA in the context of federated cloud has also been the focus of research initiatives. Such initiatives range from simulation frameworks purporting to help in selecting the optimal combination of cloud services which better meet SLA requirements [40] to the optimal negation of SLA using multi-objective genetic algorithms [41]. In a similar way, some recent work on accountability in the cloud has started to emerge through projects such as A4CLOUD (http://www.a4cloud.eu), whereby researchers are trying to devise models that can help put in place the set of mechanisms that would ensure cloud providers are hold accountable should there be a breach of SLA or a security incident that can be traced back to a lax in their security. In the context of A4Cloud the concept of transparency in the broader sense is dealt

with as an attribute of Accountability [42]. Readers interested in further comprehending the scope and diversity of existing efforts on SLA-based monitoring of cloud security can refer to the taxonomy of Petcu [43].

The major problem with the adoption of SLA management as a means to enhance security transparency is primarily its practicality. Indeed the academic notion of SLA appears to be far more extensive than it is in reality. During the course of this work, the authors have approached a number of CSPs based in Luxembourg with the aim to get a glimpse on the set of items that were included in their SLA specifications. Most often, such documents were restricted to aspects such as allocated bandwidth, storage capacity, etc.., while the only security aspect included was related to service availability. Clearly, the items included in those specifications were those the companies were confident they could deliver on. Their argument on the most pressing and challenging issues such as security was that stringent and redundant mechanisms were in place for its guarantee, as witnessed by some of their security certification.

Security certification and audits

Amongst the threats listed in Tables 2 and 3, Threat 7 is perhaps the one that cannot be resolved with technical means alone as it involves mutual trust considerations between the CSP and the CSC. Furthermore, as already mentioned, the security level of a cloud service is dependent on several factors, including the security of the CSP and all other CSCs using the service. In the cloud, such a complexity can be further increased due to the federation of an application's component across different cloud providers [44] and to the fact that very often the complete chain of CSP-CSC involved in the provisioning of one's service is not always known to the CSC.

In their effort to reduce the fears of the CSCs and distinguish themselves from competitors by promoting their service as one that is secure, CSPs have often turned to certifications as a way of swaying CSCs. Reasons for this include the lack of metrics and sometimes resources from the CSC to adequately assess the cloud services. As such certification from a third party organization has been hailed by proponents as the ultimate means of promoting trust and transparency in the cloud ecosystem, which is a key to its wider acceptance [45]. For instance, certification to ISO/IEC 27001 is valued in the industry, as it provides a holistic framework for appreciating how well a company manages its information security. The standard emphasises the need for organisations to have clear means of understanding their security needs. Additionally it is meant to assist them in implementing controls to address risks facing their business and monitoring, reviewing and improving the performance and effectiveness of the Information Security Management Systems (ISMS). Importantly, the authors in [45] have also highlighted the need for certification scheme to be affordable to avoid smaller company having the carry those expenses in the price of their service delivery and thus become ultimately uncompetitive against their bigger rivals.

Following the argument that providers should rely more on a certification from a governing or standardised institution that stipulates the provider has established adequate internal security controls that are operating efficiently, the Cloud Security Alliance has made a number of effort towards the provision of clear guidelines towards controlling security risks in the cloud [18]. The CSA guidance is made up of 99 control specifications covering such area as: Compliance, Governance, Facility, human resource and Information security, Legal matters, Operations, Risk and Release management, Resiliency and the security architecture. The individual controls identified within the guideline emanate from well-established standards and guidelines pertinent in both the context of traditional Information Systems and the cloud, covering a wide range of domains including the IT Governance (COBIT), the banking and financial domain (PCI-DSS and BITS), Government (NIST SP800-53 and FedRAMP), Health care (HIPAA) and cross-domain standard for the management of information security systems (ISO/IEC27001). Recently, the CSA has put forward the idea of a three-levelled certification scheme that would rely on the compliance to its set of security guidance and control objectives [16–18, 46]. According to the CSA each level will provide an incremental level of trust to CSP operations and a higher level of assurance to the CSC.

The first of such levels (which it must be stressed is a mere self-assessment exercise) requires each CSP to submit a report on the CSA to assert its level of compliance to the advocated best practices. The second level, referred to as *CSA STAR CERTIFICATION*, is meant to provide a third-party independent assessment conducted by an approved certification body under the supervision of the CSA and BSI. The third level will extend the *STAR CERTIFICATION* in view of providing a continuous monitoring based certification.

Similarly, the Certified Cloud Service of TÜV Rheinland, runs a certification scheme which is based on CSPs compliances on the most essential information security standards such as ISO 27001 basic protection standards issued by the German Federal Office for Information Technology and ITIL [47].

It is clear that standardization and certification bodies are rushing to make a footprint in the certification market related to cloud based services. Although the intention lies in helping to make an informed judgment about the quality of a given CSP, companies with interest in adopting the cloud could be swamped and confused by the sheer number of standards and their actual scope. In anticipation to

this, recent research conducted by the University of Cologne in Germany has suggested a taxonomy of cloud certification whereby commonly agreed structural characteristics of cloud service certifications could be adopted as a baseline for classifying certification schemes depending on their core purpose [48].

The adoption of certification as a way of making a statement about the reliance of the security of one's service has reinforced the importance of audits for the cloud model. Audits are meant to provide a third party independent assessment of the posture of the security.

Until autumn 2011, the SAS70 was a standard audit approach for service companies to use with their customers instead of customers individually auditing the services companies [49]. The actual purpose of the standard was primarily aimed to assess the sufficiency and the effectiveness of the security controls of the CSP. The standard was superseded by SSAE16 (www.ssae16.com), which stands for Statement on Standards for Attestation Engagements No. 16. The rationale for such a changed was to align the reporting standard of US based companies to that of the international standard ISAE3402 (http://isae3402.com/). One of the core difference between the two standards rests on the fact that the evaluated company is bound to provide a written statement about the accuracy of the description of their system and the corresponding time frame during which such an assessment has been made.

What becomes apparent after analyzing the different audit standards available is that they rely in a large part on the words and assessment of the CSP. Such information cannot be guaranteed to be immune from bias. For instance, the CloudAudit initiative from the CSA (http://cloudaudit.org/CloudAudit/Home.html) is seeking to provide a common API for CSPs to specify their assertion, assessment and assurance. Such information is meant to be made readily available to the CSCs and also allow the latter to make comparisons between potential providers based on their security. Given the CSP has often a greater control over the security in the cloud, with very little visibility (if any) for the CSC, the frequency and independence of such audits is paramount along with the appropriate reporting of the findings to the CSC. Thus automated and continuous audits will be more appropriate, especially when considering the evolving nature of the cloud infrastructure.

The importance and difficulty with encryption of data as means of establishing assurance in the cloud

Encryption has been seen as a natural solution for ensuring the integrity and confidentiality of data in the cloud. Indeed, it was meant to guarantee that data in transit or stored by cloud providers are not tampered with, or looked at, by a third party (whether internal to the CSP or external). However, until recently, encryption was no silver bullet to this problem. Indeed, the peculiarity of the cloud model (namely the devolution of the data storage and management to the CSP), means it is hard to readily apply traditional cryptographic methods for data security and privacy protection [50, 51].

One of the well-known challenges relating the effective usage of encryption in the cloud is key management. According to the Cloud Security Alliance, three main imperatives need to be met [17]. The first concerns the security of the key stores in order to avoid compromising all encrypted data. Then comes the actual policing of the access to those keys; to ensure only legitimate users get access to the keys, and the implementation of a clear policy to ensure keys are not stored by the entity meant to be using them. Finally, ensure that safe backups exist for data recovery in case of key loss. Nonetheless there are signs that things are moving on that side as the advancement on order preserving encryption and database systems have facilitate the emergence of application where the cryptographic key remains at the client [52].

Some authors, such as Anthes and Zhu et al., have also highlighted the difficulty of effectively applying encryption in a cloud realm [1, 53]. According to these authors, it all comes down to the difficulty to process encrypted data without a-priori having to decrypt them, and the necessity to download a local copy of data - which can be an expensive transaction, especially for large-size files. The good news, however, is that research in cryptography is now starting to catch up, even if an efficient and full applicability to complex real life cloud applications is still years ahead according to practitioners [1]. Interestingly, some of the big players in the cloud market are leading those initiatives.

The work of IBM's Craig Gentry on a fully homomorphic encryption scheme, which uses ideal lattices, has provided a hope of processing some data without initially having to decrypt them [54]. Using a homomorphic encryption in general, the result of computations on the encrypted data is itself the encryption of the computation on the plain text. A fully homomorphic encryption extends partial homomorphic encryption by supporting the homomorphic computations of both addition and multiplication on the plain data, making it more powerful. Since the actual scheme does not decrypt itself, the entity handling the data does not have any knowledge of the original data. A recent application of the work on fully homomorphic encryption include the initiative of López-Alt et al. in [55] who introduced the notion of on the fly *multiparty computation* or MPC. This is achieved using a new type of encryption scheme referred to as *multikey FHE*, which is capable of operating on inputs encrypted under multiple, unrelated keys. Although fully homomorphic encryption is pertinent to storage at an untrusted CSP, the computational cost is considered so important

that its current applicability in a real context remain years away [1].

Microsoft's Kamara and Lauter have defined an architecture that combines some cryptographic primitives in view of providing secure cloud storage [56]. The precept of their virtual private storage service is that the cloud service provider is not completely trustworthy. Using such a service on top of a public cloud purports to ensure the confidentiality and integrity of the data. The virtual private storage service proposed is made of three main components: the *data processor*, the *data verifier* and the *Token generator*. The *data processor* encrypts and encodes the data and metadata, with a variety of cryptographic primitives such as symmetric encryption scheme, attribute-based encryption and searchable encryption scheme. In the event that the consumer wishes to retrieve the data, the *token generator* creates a token using a tag which, references a certain file. The token is then sent to the cloud service provider who will carry out the retrieval of the corresponding encrypted files. The integrity of the data can be verified by invoking the *data verifier*. The authors refer to this mechanism as a *proof of storage*; that is, a protocol executed between a client and a server with which, the server can prove to the client that it did not tamper with its data.

Juels et al. proposed a protocol called *Proof of Retrieval (POR)* that helps users verify that large files are not deleted or modified prior to retrieval, without actually downloading the files [50]. The technique proposed consists of encrypting a given file and embedding a set of randomly-valued check blocks or *sentinels*. The data owner then challenges the entity archiving the data by specifying the positions of a collection of sentinels and asking it to return the associated sentinel values. The modification or deletion of some portion of the file will, with some probability value, affect the sentinels leading to an inaccurate response. A similar approach to POR is the *Provable Data Possession (PDP)* introduced by Atheniese et al. in [57]. The PDP also uses a probabilistic proof technique to allow the verification that an untrusted server stores a client's data as well as ensuring the authenticity of the latter. It adopts a scheme known as *Homomorphic linear Authenticator (HLA)*. Using the HLA, a file is subdivided into a number of blocks, which are then tagged in a way that, for a given vector generated as challenge for a proof of possession, the server can homomorphically construct a tag for authenticating the value of the polynomial resulting from combining the components of such a vector and the file's blocks. Several Extensions of the approach have since followed including those presented in [58, 59].

The development of techniques for verifying the integrity of data in a cloud domain has also been the focus of recent academic works. The work by Zhu et al., relies on the principle of the *POR* for ensuring the integrity and privacy of the data, but addresses also the need for such an audit to be efficient and less costly to the consumer [53]. In that respect, the authors have suggested the use of a Third Party Auditor (TPA) which can afford to periodically audit the outsourced data and make them available on-demand to the consumer; thereby avoiding the burdensome and cost associated to the data validation by downloading them locally. In practical terms, the data owner is assigned a secret key that is used to pre-process the file, which is partitioned into a certain number of blocks. A set of public verification information is then generated and stored at the TPA, before the actual file and some verification tags are transmitted to the CSP. When a request for check is issued by the data owner, the TPA uses a protocol of proof of retrievability, to issue a challenge to audit (or check) the integrity and availability of the outsourced data using the public verification information. Importantly, the overall architecture proposed by the authors can be implemented by the TPA without involving the data owner.

The work by Wang et al. has also sought to resolve the privacy concerns in third party auditing of data integrity in cloud services through the usage of the TPA [51]. The audit of the integrity still relies on homomorphic encryption. Beside the actual technique of ensuring privacy while resorting to a TPA, Wang et al. have included a batch technique that would enable the TPA to gain in efficiency when having to process numerous simultaneous request of integrity check.

Discussion and desiderata for a trusted cloud service

There is no doubt the current effort by security researchers, particularly in encryption, is promising to change the way that medium and large corporations perceive the security of cloud services. This is likely to become more so when the processing of the encrypted data without initially having to access them, as purported by fully homomorphic encryption schemes, becomes a more practical and viable solution. As cloud users can never be sure about the actual location of their data at a given time, a technique such as the *Provable Data Possession (PDP)*, can prove useful for determining whether specific storage servers possess the data. Still, more remains to be done to achieve a good level of security transparency that should help boost the confidence of the consumer on a security matter that is more and more devolved to a third party, often the CSP. Although some of the responsibilities to guarantee the security of cloud services rest with the service provider, it is also the duty of the CSC to ensure proper evidence of security is demonstrated by the CSP prior to sending sensitive and confidential information data in the cloud [15].

The current approach towards security transparency has been on the form of an agreement between the CSP and the CSC, on top of the usual SLA. Such an agreement often considers the cloud service providers liable in case a security incident that occurs in their infrastructures is not promptly reported to the consumers. Still, such a reporting may not be timely enough for the consumer as, the incident impacts may have already materialised in the midst of the CSC's service by the time of the reporting. The alternative approach adopted by the CSPs (and also advocated by entities such as the Cloud Security Alliance, ENISA and NIST) is that the CSPs should rely more on a certificate from a governing or standardised institution that stipulates the CSP has established some adequate internal security controls that are operating efficiently. The caveat remains that being certified by a standardisation body does not guarantee that one's security will remain in a good posture indefinitely. Hazards in the system's environment may arise; intentional or unintentional modification of some of the security mechanisms configurations may occur and lead to the security mechanisms being ineffective. Moreover, as multi-tenancy allows several customers to be hosted on the same underlying infrastructure, traditional audits and reviews of a CSC to give the expected level of assurance becomes less practical [4], especially given that could lead to security breaches of collocated CSCs when an untrustworthy security auditor is involved [60]. The work of Dolitszcher et al. [61] provides some hope in addressing such a gap. Indeed, the security audit as a service (SAaaS) approach proposed by the authors resort to the usage of multi-agent system (MAS) for conducting the audit of virtual machines allocated to cloud consumers dynamically. This data interpretation is achieved using a Security Service Level Agreements (SSLA) policy modelling engine, which allows the definition of monitoring events and consideration of business process flows. As agents are renowned for their autonomy and flexibility, the usage of autonomous agents appears to be suitable for the identification of anomalies in such a highly scalable environment as the cloud. In addition to this, current efforts such as encryption, SLA and Virtual machines monitoring need to be complemented by security assurance activities [62–65] that is, the continuous probing and reporting on the adequacy (correctness, effectiveness, efficiency and non-vulnerability) of the security mechanisms put in place by the CSP. Furthermore, some desiderata would need to be observed for achieving a more comprehensive Security Transparency and Mutual Audit (STMA) in the cloud. For each of those points, thereafter enumerated, we provide some initial directions that could be further investigated by the research community and the industry. Such desiderata include:

1. STMA based ranking of cloud based services:
   This would involve establishing a systematic approach that would help assess and rank cloud providers based on the adequacy of their security and the level of security transparency and audit offer to the CSC.
2. Engineering cloud services with STMA in mind:
   A point that is closely related to the one above discussed relates the elaboration of a conceptual modelling and design framework tailored to reflect the cloud realm. Amongst others the idea would be to devise interactive software engineering methods that allows capturing the expectations of the CSC in terms of STMA while allowing the CSP to suggest a design and strategy to meet such requirements.
3. Architectural design and method for enforcing security transparency and mutual auditability:
   While the first two desiderata pertain to knowledge and tools that are relevant while contemplating to outsource to the cloud, this one relates to methods and the technology require for (i) ensuring no nefarious use of the service is being undertaken by unscrupulous CSCs;(ii) continuously gathering evidence to support security, compliance and other quality of service related claim by a certain CSP and; (iii) sharing security related information with the CSC.

STMA based ranking of cloud based services

The existence of a standardized ranking scheme is essential to ensure the informed selection of a CSP that meets the CSC's STMA expectations. The challenge for achieving this resides in the definition of a ranking model and process that will enjoy a broader acceptance. An initiative in that direction includes the Complete-Auditable-Reportable or CARE approach proposed in our previous publication [65]. The approach helps to determine the adequacy of a CSP sponsored security using STMA criteria. According to CARE, the level of security trustworthiness of a given CSP is dependent on three factors, namely: (a) the assurance that the CSP may deliver a service that meets the CSC's security and privacy need, (b) whether such security can be adapted to address concerns identified during planned and frequent audits, and (c) the transparency of information regarding security of the cloud service conveyed to the CSC.

A similar initiative was suggested by Pauley [66] through the proposal of a Cloud Provider Transparency Scorecard (CPTS). Pauley's scorecard-based assessment of CSPs' transparency consists in scoring them on four different areas including security, privacy, external audits/certifications, and service-level agreements, using a set of questions provided within the ENISA and the CSA's guidelines. Relevant information on the CSP's standing on the four

mentioned areas, including publically available information about the CSP's past security woes is used as input for scoring individual questions. Boolean responses collected for each question can then be summed up to provide an overall score for transparency or a relative/percentile based score per area assessed.

For a real take up of any STMA based ranking of CSP, that enjoys the support of future CSC's, especially those from the business world and government agencies, a standardization body or government led initiative could be preferable. That is not to cast aside efforts undertaken by the research and academic community. Instead, we argue that Government and standardization bodies hold more sway over the commitment of the business world to adopt such a classification scheme. This is specially the case, if a certain level of STMA was laid by a regulation as a minimum mandatory requirement that a cloud based service ought to have for being considered by a given sector of business or government agencies.

Engineering cloud services with STMA in mind

Rather than considering STMA as an afterthought, which could be a source of conflicts (especially if some features or components need to be added to enable the automation of the audit and sharing of the security related information), an efficient way could be to consider STMA throughout the modeling and design process of Cloud based services. Furthermore it is clear that STMA requirements will be different in their specificities, as well as bearing different priorities in the eyes of different CSCs. Similarly CSPs will have different strategies in meeting those STMA requirements. Consequently, customizing the way in which STMA requirements and related solutions are specified appears to be more appropriate. For instance, an STMA-driven cloud service engineering could systematically support, on the one hand, the cloud consumers in specifying their STMA related requirements. On the other hand, providers would be able, through the methodology, to better appreciate what and how components should be put in place to deliver a service that meets the STMA requirements of a particular CSC.

Architectural design and method for enforcing mutual auditability and security transparency

Because security transparency and mutual auditability imply the possibility for the CSC or its auditors to probe the security of the CSP, it is essential that research is undertaken on the development of new architectures that would enable such introspection and the secure flow of the related information from the cloud node hosting the CSC's application or data to the relevant location for forensic analysis and decision making. The area of event computing [67, 68] offers some potential that could be exploited in that context. In fact, events provide a powerful construct to capture current state of a system (service) and deviations from expectation and to predict future security or QoS related issues [67, 68]. Additionally a well-defined architecture can support event based monitoring in ensuring the prompt dissemination of events' occurrence to the interested parties who would subsequently make judgment on the course of action to adopt. Amongst others, it may be a way to hold cloud providers accountable for a security breach that may have stemmed from a weakness in their security; a breach of SLA or other escrows between the two parties. The set of patterns and the detection algorithms associated could also constitute a powerful tool for a cloud provider concerned with abusive and nefarious use of its service by clients. Efficiently leveraging the power of events for the purpose of STMA in the cloud will entail further investigation in mainly three areas as depicted in Fig. 1:

i) Specifying STMA requirements using event constructs. A prerequisite for an effective use of event computing in enforcing STMA in cloud services includes: the definition of atomic events structure coupled with the adoption of a pattern specification language that is expressive enough to capture the realm of events of interest. While patterns of events [67] (including event counters, conjunction, disjunction and sequences of events) could be readily reuse or extended to reflect the complexity of events of interest to the cloud stakeholders, existing event specification languages such as ETALIS [69], TESLA [70] and YALES [71] are amongst the most expressive languages that can be adopted for the specification of event patterns pertinent to STMA. Furthermore, given most STMA related events would be related to security, candidate format for representing atomic events of interest may include the Extensible Configuration Checklist Description Format - XCCDF [72] and the Intrusion Detection Message Exchange Format- IDMEF (http://www.rfc-base.org/txt/rfc-4765.txt), both being an XML based format. While IDMEF is intended to be a standard data format that automated intrusion detection systems can use to report alerts about events that they deem suspicious, XCCDF is used to specify security checklists and benchmarks amongst others. The overarching purpose of the format is to provide a uniform expression of security checklists, benchmarks, and other configuration guidance, and thereby foster more widespread application of good security practices. Another advantage of the format includes the reuse of some existing Security Content and Automation Protocol (SCAP) [73] tools for the detection of atomic events.

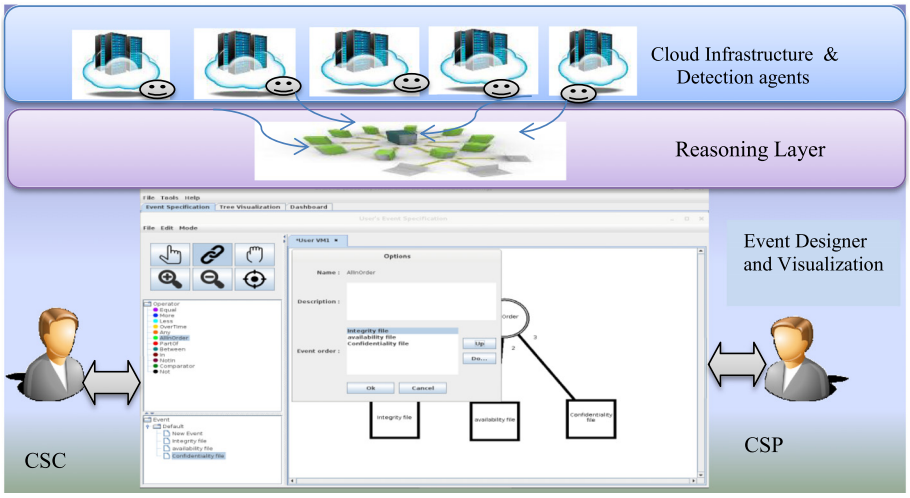

Fig. 1 High level Architecture for STMA enforcement

ii) The elaboration of a multi-agent system embedded within the cloud infrastructure (CI) with the purpose of detecting atomic events specified within the STMA event specification platform that we refer to as Event Designer. The elaboration and management of the detection agents may be performed using JADE platform [74]. Challenges associated to this include ensuring that software agents entrusted with probing and retrieving the security information are not corrupted at the CSP's, or that the collected information does not fall in the wrong hands. What information may be shared with a given consumer and its extent should be contractually stipulated in a STMA based agreement that could be part of a global service level agreement between the two parties.

iii) Upon the detection of atomic events by the embedded agents, another layer of processing would be required to determine whether a pattern of events specified by either the CSC or CSP within an event specification platform (STMA Event designer) has materialized. Such a detection layer could intertwine both a specific architecture for atomic event processing such as Storm [75] along with algorithms for detecting each of the patterns specified by the CSC/CSCP.

Conclusion

As the cloud paradigm has been gaining momentum, so have the concerns about its security and privacy. Nonetheless, the security community has been devising solutions that may help to thwart some of the security challenges. In this vein of effort, novel encryption mechanisms, SLA and virtual machines monitoring have been amongst the most researched topics. However, what can be taken from this analysis of the current security practices is that the current research has often overlooked the importance of mutual trust considerations and the need for mutual auditability in the cloud.

By shedding more light on the current security practices and discussing on how they fare in addressing the lack of security transparency and mutual auditability in the cloud, the authors hope to stimulate more research in that direction. The desiderata discussed in the previous section of the paper give a flavour of some of the challenges that await researchers keen on filling the existing gap.

Competing interests

The authors declare that they have no competing interests.

Authors' contributions

MO drafted the manuscript, carried out the background work to identify the shortcomings in current initiatives dealing with security transparency. He also identified the number of desiderata that could be heeded by the research community to promote more security transparency in the cloud. SM and HC have contributed in the analysis of security assurance work in the cloud that ultimately led to the paper. SF and ED have primarily contributed to the orientation of the paper, its writing up and finalisation. All authors have contributed in the write up and finalisation. All authors read and approved the final manuscript.

Acknowledgements

This work has been conducted in the context of the SAINTS project, financed by the national fund of research of the Grand Duchy of Luxembourg (FNR). Under grant number C12/IS/3988336. The authors also thanks Reijo Savola from VTT for his insights into cloud security concerns.

Author details

[1]Luxembourg Institute of Science and Technology, Esch/Alzette L-4362, Luxembourg. [2]The Centre for Security, Communications and Network Research, Plymouth University, Plymouth, UK.

Received: 2 June 2014 Accepted: 14 May 2015
Published online: 02 June 2015

References

1. Anthes G (2010) Security in the cloud. Communication of the ACM 53(11):16–18, ACM digital library, New York
2. Schneier B (2009) Cloud computing. Accessed 11th February, 2014 from http://www.schneier.com/blog/archives/2009/06/cloud_computing.html
3. Horch A, Christmann C, Kett H, Falkner J, Anette Weisbecker A (2013) Essential Elements of an SME-specific Search of Trusted Cloud Services. In: Proceedings of CLOSER. Springer, Heidelberg, pp 88–94
4. Dorey P.G., Leite A. (2011) Commentary: Cloud computing – A security problem or solution? Information Security Technical Report, 16 (3–4), pp. 89–96, Elsevier
5. El-Gazzar RF (2013) Cloud Computing Adoption Factors and Processes for Enterprises - A Systematic Literature Review. In: Proceedings of CLOSER. Springer, Berlin, pp 78–87
6. Subashini S, Kavitha V (2011) A survey on security issues in service delivery models of cloud computing. J Netw Comput Appl 34(1):1–11, Elsevier
7. Lombardi F, Di Pietro R (2011) Secure virtualization for cloud computing. J Netw Comput Appl 34(4):1113–22, Elsevier
8. Rodero-Merino L, Vaquero LM, Caron E, Muresan A, Desprez F (2012) Building safe PaaS clouds: a survey on security in multitenant software platforms. Computers & Security 31(1):96–108
9. Vaquero LM, Rodero-Merino L, Morán D (2011) Locking the sky: a survey on IaaS cloud security. Computing 91(1):93–118, Springer, Vienna
10. Chen Y, Paxson V, Katz RH (2010). What's New About Cloud Computing Security? Report EECS Department, University of California, Berkeley. Accessed September 13, 2012 from http://www.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.html
11. Hu F, Qiu M, Li J, Grant T, Tylor D, McCaleb S, Butler L, Hamner R (2011) A review on cloud computing: design challenges in architecture and security. J Comput Info Technol 19(1):25–55
12. Popović K, Hocenski Z (2010) Cloud computing security issues and challenges. In: Proceedings of the 33rd International Convention. IEEExplore, Opatija, pp 344–349
13. Oza NV, Karppinen K, Savola R (2010) User Experience and Security in the Cloud – An Empirical Study in the Finnish Cloud Consortium. In: Proceeding of CloudCom. IEEExplore, Indianapolis, pp 621–628
14. Jansen W, Grance T (2011) Guidelines on Security and Privacy in Public Cloud Computing, NIST SP 800–144. National Institute of Standardisation and technology, Gaithersburg
15. Teneyuca D (2011) Internet cloud security: the illusion of inclusion. Info Security Technical Report 16(3–4):102–7, Elsevier
16. Cloud Security Alliance (2010) Top Threats to Cloud Computing. Accessed 21 March 2014 from https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf
17. Ouedraogo M, Islam S (2015) Towards the Integration of Security Transparency in the Modelling and Design of Cloud Based Systems, In proceedings of CAiSE Workshops 2015: 495-506, Lecture Notes in Business Information Processing Springer International Publishing Switzerland.
18. Cloud Security Alliance –CSA (2011). Cloud Controls Matrix v.1.3, Accessed 23rd March 2014 from: https://cloudsecurityalliance.org/
19. Gellman R (2009) Privacy in the clouds: risks to privacy and confidentiality from cloud computing. Report, World Privacy Forum (WPF)
20. Cloud Security Alliance (2011) Security guidance for critical areas of focus in cloud computing V3.0, Accessed 20rd October, 2014 from http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf
21. Cloud Security Alliance. (2009) Security guidance for critical areas of focus in cloud computing V2.1.0, Accessed 18rd March, 2014 from http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf
22. Santos N, Gummadi KP, Rodrigues R (2009) Towards Trusted Cloud Computing. In: Proceedings of the 2009 conference on Hot topics in cloud computing (HOTCLOUD). USENIX, San Diego
23. Brodkin J. (2009) Cloud computing outages: Amazon customers the latest to suffer downtime. Accessed 12th March 2014 from: http://www.networkworld.com/community/node/48961
24. Cloud Security Alliance. (2013) The Notorious Nine Cloud Computing Top Threats in 2013. Accessed 20 October 2014 from https://cloudsecurityalliance.org/download/the-notorious-nine-cloud-computing-top-threats-in-2013/
25. Mills E. (2012) Cybercriminals move to the cloud, Accessed 12th December, 2013 from: http://news.cnet.com/8301-1009_3-57464177-83/cybercrime-moves-to-the-cloud/
26. McAfee and Guardian Analytics. (2012) Dissecting Operation High Roller. Accessed 10 February 2014 from: http://www.mcafee.com/mx/resources/reports/rp-operation-high-roller.pdf
27. Srinivasan MK, Sarukesi K, Rodrigues P, Manoj SM, Revathy P (2012) State-of-the-art cloud computing security taxonomies: a classification of security challenges in the present cloud computing environment. In: Proceeding of ICACCI. ACM digital library, New York, pp 470–476
28. Winkler V. (2011) Securing the cloud- cloud computer security techniques and tactics. Syngress
29. Garfinkel T., Pfaff B, Chow J, Rosenblum M, Boneh D. (2003) Terra: a virtual machine-based platform for trusted computing. In: Proceedings of SOSP 2003, ACM
30. Krautheim FJ (2009) Private Virtual Infrastructure for Cloud Computing. In: Proceedings of the HOTCLOUD conference 2009. ACM, New York
31. Arshad J, Townend P, Jie X (2009) Quantification of Security for Compute Intensive Workloads in Clouds. In: Proceedings of the 15th International Conference on Parallel and Distributed Systems. IEEE, Shenzhen
32. De Chaves SA, Uriarte RB, Westphall CB (2011) Towards an architecture for monitoring private clouds. IEEE Commun Mag 49(12):130–7, IEEE
33. Savola R, Juhola A, Uusitalo I (2010) Towards wider cloud service applicability by security, privacy and trust measurements. In: Proceedings of the 4th Int. Conf. on Application of Information and Communication Technologies (AICT'10). IEEE, Tashkent, pp 45–50
34. Rak M, Liccardo L, Aversa R (2011) A SLA-based interface for security management in cloud and GRID integrations. In: Proceedings of the 7th International Conference on Information Assurance and Security (IAS). IEEE, Melaka, pp 378–383
35. Rak M, Luna J, Petcu D, Casola V, Suri N, Villano U. (2013) Security as a Service Using an SLA-based Approach via SPECS. In:Proceedings of IEEE 5th International Conference on Cloud Computing Technology and Science (CloudCom), pp, 1 – 6, IEEE
36. Wieder P, Butler JM, Theilmann W, Yahyapour R (eds) (2011) Service Level Agreements for Cloud Computing. Springer-Verlag, New York
37. Lorenzoli D, Spanoudakis G (2010) EVEREST+: Runtime SLA Violations Prediction. In: Proceedings of the 5th Middleware for Service-oriented Computing Workshop. ACM, New York
38. Shanahan M (1999) The event calculus explained. In Artificial Intelligence LNAI 1600:409–30
39. Chazalet A (2010) Service level checking in the cloud computing context. In: Proceedings of the third International Conference on Cloud Computing. IEEE, Miami, pp 297–304
40. Kohne A, Spohr M, Nagel L, Spinczyk O (2014) FederatedCloudSim: a SLA-aware federated cloud simulation framework. Proceedings of the 2nd International Workshop on CrossCloud Systems, ACM, New York
41. Maity S, Chaudhuri A (2014) Optimal negotiation of SLA in federated cloud using multiobjective genetic algorithms. In: Proceedings of CLOUDNET 2014. IEEExplore, New York, pp 269–271
42. Nuñez D, Fernandez – Gago C, Pearson S, Felici M. (2013) A Metamodel for Measuring Accountability Attributes in the Cloud. In: Proceedings of the 2013 IEEE International Conference on Cloud Computing Technology and Science (CloudCom 2013), IEEE
43. Petcu D (2014) A taxonomy for SLA-based monitoring of cloud security. COMPSAC 2014:640–1
44. Rodero-Merino L, Vaquero LM, Gil V, Galán F, Fontán J, Montero RS, Llorente IM (2010) From infrastructure delivery to service management in clouds. Future Generation of ComputerSystems 26(8):1226–40
45. Sunyaev A, Schneider S (2013) Cloud services certification. Communication of the ACM 56(2):33–36, ACM digital Library, New York
46. Cloud Security Alliance –CSA. (2012). Consensus Assessments Initiative Questionnaire 1.1. Available at: https://cloudsecurityalliance.org
47. TÜV Rheinland's. (2014) certification for cloud providers, Accessed on 20th October 2014 from: //www.tuv.com/en/corporate/business_customers/information_scuriy_cw/strategic_information_security/cloud_security_certification/cloud_security_certification.html
48. Schneider S, Lansing J, Gao F, Sunyaev A (2014) A Taxonomic Perspective on Certification Schemes: Development of a Taxonomy for Cloud Service Certification Criteria. In: Proceedings of the 47th Hawaii International Conference on System Sciences (HICSS 2014). IEEE, Waikoloa
49. AICPA. (2012) Statement on Auditing Standards (SAS) n°70. Accessed October 20, 2013. from http://sas70.com/sas70_overview.html

50. Juels A, Kaliski BS Jr (2007) Pors: proofs of retrievability for large files. In: Proceedings of the 2007 ACM Conference on Computer and Communications Security (CCS 2007). ACM Digital library, New York, pp 584–597
51. Wang C, Wang Q, Ren K, Lou W (2010) Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing. In: Proceedings of the 29th conference on Information Communications (INFOCOM 2010). IEEE, San Diego, pp 525–533
52. Kerschbaum F.(2013) Searching over encrypted data in cloud systems, in: Proceedings of SACMAT 2013, pp.87-88, ACM ditigal library
53. Zhu Y, Hu H, Ahn GJ, Yau SS (2012) Efficient audit service outsourcing for data integrity in clouds. J Syst Softw 85(5):108–1095, Elsevier
54. Gentry C (2009) Fully Homomorphic Encryption Using Ideal Lattices. In: Proceedings of the 41st annual ACM Symposium on Theory of Computing (STC 2009). ACM, NewYork, pp 169–178
55. López-Alt A, Tromer E, Vaikuntanathan V (2012) On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption. In: Proceedings of STOC 2012. ACM, New York, pp 1219–1234
56. Kamara S, Lauter K (2010) Cryptographic cloud storage. In: Proceedings of Financial Cryptography. Workshop on Real-Life Cryptographic, Protocols and Standardization, Springer, Heidelberg
57. Ateniese G, Burns R, Curtmola R, Herring J, Kissner L, Peterson NJZ, Song D (2007) Provable Data Possession at Untrusted Stores. In: Proceedings of CCS'07, Alexandria, VA. ACM, New York, pp 598–609
58. Shacham H, Waters B (2008) Compact proofs of retrievability. In: Advances in Cryptology (Asiacrypt '08), vol. 5350, Lecture Notes in Computer Science. Springer, Heidelberg, pp 90–107
59. Dodis Y, Vadhan S, Wichs D (2009) Proofs of retrievability via hardness amplification. In: Theory of Cryptography Conference, vol. 5444 of Lecture Notes in Computer Science. Springer, Heidelberg, pp 109–127
60. Rübsamen T., Reich C. (2013) Cloud Audits and Privacy Risks. In: Proceedings of OTM conferences, LNCS V8185, pp 403–4013, Springer
61. Doelitzscher F, Reich C, Knahl M, Clarke N (2012) An agent based business aware incident detection system for cloud environments. Journal of Cloud Computing:Advances, Systems and Applications 1(9):1–19, Springer-Verlag, Berlin
62. Ouedraogo M, Mouratidis H, Hecker A, Bonhomme C, Khadraoui D, Dubois E, Preston D (2011) A new approach to evaluating security assurance. In: Proceedings of the 7th International Conference on Information Assurance and Security (IAS). IEEExplore, New York, pp 215–221
63. Ouedraogo M, Savola R, Mouratidis H, Preston D, Kadraoui D, Dubois E (2013) Taxonomy of quality metrics for assessing assurance of security correctness'. Softw Qual J 21(1):67–97, Springer, US
64. Ouedraogo M, Khadraoui D, Mouratidis H, Dubois E (2012) Appraisal and reporting of security assurance at operational systems level. Journal of software and system and software 85(1):193–208, Elsevier
65. Ouedraogo M, Mouratidis M. (2013) Selecting a cloud service provider in the age of cybercrime, Computers & Security, vol.38, pp.3-13 Special issue on Cybercrime in the Digital Economy, Elsevier
66. Pauley W (2010) Cloud provider transparency: an empirical evaluation. IEEE Security & Privacy 8(6):32–3, IEEExplore, New York
67. Etzion O., Niblett P. (2010) Event Processing in Action. Manning Publications Company 2010, ISBN 978-1-935182-21-4, pp. I-XXIV, 1–360
68. Luckham DC (2005) The power of events - an introduction to complex event processing in distributed enterprise systems. ACM, New York, p I-XIX, 1–376. ISBN 978-0-201-72789-0
69. Anicic D, Rudolph S, Fodor P, Stojanovic N (2012) Real-time complex event recognition and reasoning-a logic programming approach. Appl Artif Intell 26(1–2):6–57
70. Cugola G, Margara A (2012) Complex event processing with T-REX. J Syst Softw 85(8):1709–28
71. Zhang RJ, Unger EA (1996) Event Specification and Detection, technical report. University, Kansas State
72. Waltermire D, Schmidt C, Scarfone K, Ziring N (2011) Specification for the Extensible Configuration Checklist Description Format (XCCDF) Version 1.2. National Institute of Standards and Technology, Gaithersburg, MD, pp 20899–893
73. Waltermire D, Quinn S, Scarfone K, Halbardier A (2009) The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.2., Special Publication 800–126. NIST, Gaithersburg
74. Bellifemine F, Caire G, Poggi A, Rimassa G (2008) JADE: A software framework for developing multi-agent applications. lessons learned. Information & Software Technology 50(1–2):10–21
75. Leibiusky J., Eisbruch G., Simonassi D. (2012) Getting Started with Storm, O' Reilley