From Security to Assurance in the Cloud: A Survey

CLAUDIO A. ARDAGNA, Università degli Studi di Milano, Italy
RASOOL ASAL, ETISALAT BT Innovation Center, Khalifa University, UAE
ERNESTO DAMIANI, Università degli Studi di Milano, Italy, ETISALAT BT Innovation Center, Khalifa University, UAE
QUANG HIEU VU, ETISALAT BT Innovation Center, Khalifa University, UAE

The cloud computing paradigm has become a mainstream solution for the deployment of business processes and applications. In the public cloud vision, infrastructure, platform, and software services are provisioned to tenants (i.e., customers and service providers) on a pay-as-you-go basis. Cloud tenants can use cloud resources at lower prices, and higher performance and flexibility, than traditional on-premises resources, without having to care about infrastructure management. Still, cloud tenants remain concerned with the cloud's level of service and the non-functional properties their applications can count on. In the last few years, the research community has been focusing on the non-functional aspects of the cloud paradigm, among which cloud security stands out. Several approaches to security have been described, and summarized in general surveys on cloud security techniques. The survey in this paper focuses on the interface between cloud security and cloud security assurance. First, we provide an overview of the state of the art on cloud security. Then, we introduce the notion of cloud security assurance and analyze its growing impact on cloud security approaches. Finally, we present some recommendations for the development of next-generation cloud security and assurance solutions.

Categories and Subject Descriptors: C.2.4 [**Computer-Communication Networks**]: Distributed Systems; D.2.11 [**Software Engineering**]: Software Architecture; K.6.5 [**Management of Computing and Information Systems**]: Security and Protection

General Terms: Security, Verification

Additional Key Words and Phrases: Assurance, Cloud computing, Security, Survey, Transparency

ACM Reference Format:
Claudio A. Ardagna, Rasool Asal, Ernesto Damiani, and Quang Hieu Vu, 2014. From Security to Assurance in the Cloud: A Survey. *ACM Comput. Surv.* , , Article (August 2014), 48 pages.
DOI: http://dx.doi.org/10.1145/0000000.0000000

1. INTRODUCTION

Cloud computing supports a vision of IT where resources and services are provided on demand on a pay-as-you-go basis [Armbrust et al. 2009; 2010]. It provides infrastructure, platform, and software services – known as IaaS, PaaS, and SaaS, respectively [Mell and Grance 2011] – lowering the effort needed to manage computational infrastructures. Experience has shown that the cloud can make IT cheaper, simpler, flexible, and accessible to everyone without requiring the expertise needed to own, op-

This work was partly supported by the EU-funded projects CUMULUS (contract n. FP7-318580) and by the Italian MIUR project SecurityHorizons (c.n. 2010XSEMLC).
Author's addresses: C.A. Ardagna and E. Damiani, Dipartimento di Informatica, Università degli Studi di Milano, via Bramante 65, 26013 – Crema (CR), Italy; R. Asal, E. Damiani, and Q.H. Vu, ETISALAT BT Innovation Center, Khalifa University, 127788 Abu Dhabi, UAE.

DOI: http://dx.doi.org/10.1145/0000000.0000000

erate, and manage traditional on-premises systems. Cloud customers are free to focus on service development, while cloud providers can concentrate on management activities providing an infrastructure that gives to customers the *illusion of* the availability of infinite resources [Ardagna et al. 2012].

Even though cloud computing provides all these benefits, a number of potential users are still reluctant to adopt it. Cloud computing in fact makes service providers and customers lose, at least partly, control over the status of their data and applications, impairing their ability to assess risks. According to several surveys conducted by cloud computing service providers, security solution providers, and independent researchers [Al Morsy et al. 2010; Armour et al. 2013; Ballabio 2013; Bhadauria and Sanyal 2012; Bisong and Rahman 2011; Bohli et al. 2013; Chen et al. 2010; Ibrahim et al. 2010; Kalloniatis et al. 2013; Kaufman 2010; Mansfield-Devine 2008; Muttik and Barton 2009; Pearson 2013; Ren et al. 2012; Rong et al. 2013; Ryan 2013; Sengupta et al. 2011; Srinivasan et al. 2012; Subashini and Kavitha 2011; Xiao and Xiao 2013; Younis et al. 2013], perceived lack of security is one of the main reasons discouraging customers and business owners from adopting cloud solutions.

In the last few years, the security research community has worked hard to improve the security of the cloud infrastructure and the trust of cloud users that their applications and information are correctly managed and protected. However, the proliferation of ad hoc security solutions that target a very small part of the whole problem makes a fair and sound evaluation of the state of the art in cloud security difficult. Here, we start from the notion that the cloud computing paradigm can be fully exploited only if the involvement of customers and service providers in security management is widened, increasing their trust. Following this notion, software security assurance techniques enhance cloud transparency [Ardagna et al. 2014], and increase the confidence of the cloud actors that the cloud and its services behave as expected. In line with standard software security assurance definitions [IATAC and DACS 2007], cloud security assurance can be defined as *the way to gain justifiable confidence that infrastructure and/or applications will consistently demonstrate one or more security properties, and operationally behave as expected despite failures and attacks*. Assurance is a much wider notion than security, as it includes methodologies for collecting and validating evidence supporting security properties. In this survey, we analyze the cloud security state of the art focusing on the emergence of cloud security assurance (cloud assurance for brevity). We define a taxonomy of cloud security/assurance, and provide an analysis of *i)* cloud security techniques and *ii)* corresponding assurance processes. We also provide an overview of the results of our survey. Finally, we discuss some recommendations for the design and development of next-generation cloud security/assurance techniques.

The remainder of this survey is structured as follows. Section 2 describes the taxonomy and methodology at the basis of the survey. Section 3 presents cloud-specific vulnerabilities, threats, and attacks. Section 4 provides an overview of existing security solutions. Section 5 discusses assurance techniques for cloud security verification, testing, monitoring, and certification. Section 6 presents a summary of the survey results on the basis of the proposed methodology, highlights our recommendations for next-generation security and assurance solutions, and draws our conclusions. Finally, to provide a complete and up-to-date survey of cloud security and assurance issues, challenges, requirements, and solutions, Appendix A covers additional papers that span more than one category identified in Section 2, Appendix B presents a summary of all reviewed papers according to the methodology described in Section 2,[1] Appendix C

[1]We note that summary tables (i.e., Tables I, II, III) in the paper and results in Section 6.1 refer to all reviewed papers summarized in Appendix B.

compares the survey in this paper with previous surveys and whitepapers on cloud security, discussing its originality and added value, and Appendix D describes standards for cloud security and gives an overview of research projects on cloud security.

2. METHODOLOGY

We first discuss the criteria adopted for the selection of the papers reviewed in this survey. We then describe our cloud security taxonomy that consists of three main categories and is based on the *when*, *where*, *what*, and *how* approach introduced in [Buckley et al. 2005].

2.1. Selection criteria

Our survey takes an approach different from the one followed by existing surveys in similar areas (see Appendix C). We claim that cloud paradigm development involved three major phases. The first phase coincided with the set up of the cloud infrastructure, and included the design and development of all functional aspect of clouds. The results of this effort led to the implementation of current cloud protocol stacks. The second phase moved from functional to non-functional properties and focused on the design and development of techniques for management of cloud security, dependability, and performance. Finally, the third (and current) phase coincides with the move to assurance. Assurance techniques for the cloud are aimed at verifying, proving, and guaranteeing non-functional properties of cloud-based processes and applications. In this survey, we present an overview of approaches to cloud security and assurance, identifying existing trends and highlighting gaps that have to be addressed to foster cloud adoption in security-critical scenarios. Given the huge amount of literature, we identified the following set of selection criteria.

— *Coverage*: paper selection was as inclusive as possible. We reviewed security solutions that address all security requirements relevant to the cloud and discussed security mechanisms for all levels of the cloud protocol stack.
— *Actionability*: papers were selected on the basis of the impact on concrete solutions and final products. This choice allowed us to identify what can be really implemented and integrated in real systems today.
— *Timeliness*: paper selection spanned nearly a decade, considering also solutions provided in the early years of the cloud infrastructure definition. However, to make the survey up-to-date, we introduced the criterion of timeliness, which favored the selection of papers published in recent years. This choice has been made to facilitate the selection of approaches defined in a period where the cloud computing infrastructure reached a good level of maturity and stability. Solutions presented in the early years of the cloud in fact could be unstable or not applicable in current cloud environments. In addition, the trend of cloud security publications between 2008-2012 clearly shows that most of the security-related papers were presented after 2010 [Fernandes et al. 2013].
— *Quality*: paper selection followed a strict quality evaluation. To this aim, scientific and archival publications were privileged, further favoring papers in ACM, IEEE, and Elsevier journals and conferences.

2.2. Cloud security and assurance taxonomy

Besides following sound selection criteria, a survey must provide careful organization of the reviewed material. We started by identifying some key aspects of security and assurance corresponding to major security properties [Irvine and Levin 1999; Focardi et al. 2004]. The version given below is taken from [Anisetti et al. 2013b]:

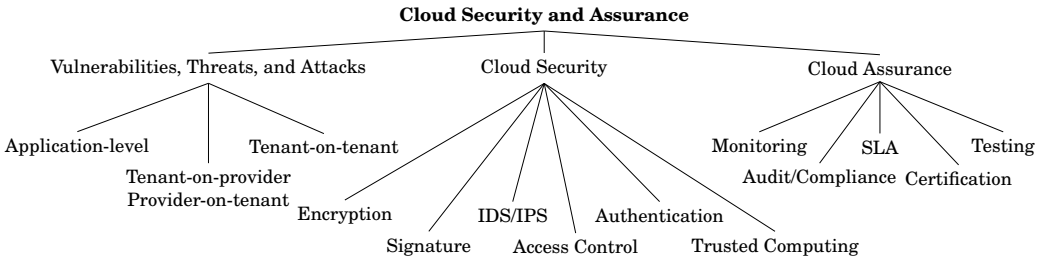

Fig. 1. Cloud security and assurance taxonomy

— *Confidentiality*: the capability of limiting information access and disclosure to authorized clients only.
— *Integrity*: the capability of preserving structure and content of information resources.
— *Availability*: the capability of guaranteeing continuous access to data and resources by authorized clients.
— *Authenticity*: the capability of ensuring that clients or objects are genuine.
— *Privacy*: the capability of protecting all information pertaining to the personal sphere of users.

Furthermore, our analysis considered three main categories of contributions (Figure 1): *i)* papers presenting new security *vulnerabilities*, *threats*, and *attacks* in the cloud, *ii)* papers presenting novel *security* techniques and mechanisms protecting data and application security in the cloud, *iii)* papers presenting original *assurance* techniques, which are used to verify, prove, and guarantee the properties provided by the implemented security techniques and mechanisms.

Security attacks are further refined in three macro-areas by specifying the attack surface: *i) application-level*, where attacks can be made by any cloud actor and target the SaaS level, including its services and data, *ii) tenant-on-tenant*, where attacks are made by malicious cloud tenants on other cloud tenants, and target the PaaS and IaaS levels, including their resources, processes, and data, *iii) provider-on-tenant* and *tenant-on-provider*, where attacks are made by malicious cloud providers (tenants, resp.) on target tenants (cloud providers, resp.) and target the IaaS level, including its resources, processes, and data. Our classification of security techniques is further refined in six macro-areas depending on the implemented security mechanisms: *i) encryption*, *ii) signature*, *iii) Intrusion Detection System (IDS)/ Intrusion Preventions System (IPS)*, *iv) access control*, *v) authentication*, *vi) trusted computing*. Assurance techniques can be used at all layers of the cloud stack to prove the security claims made by a provider on its security mechanisms and can be further refined in five macro-areas: *i) testing*, *ii) monitoring*, *iii) certification*, *iv) audit/compliance*, *v) Service Level Agreement (SLA)*. All macro-areas are aimed at increasing the trust of the users in the cloud and giving them an increased capability of evaluating the security status of the cloud stack where their applications/data reside.

2.3. When, Where, What, How

Finally, we complemented our aspects and contribution categories with labels describing the contributions' spatio-temporal coordinates. Starting from the work in [Buckley et al. 2005], we adapted the four dimensions *when*, *where*, *what*, and *how* to present a clear picture of the evolution of security and assurance solutions in the cloud. In particular, our analysis specifies when, where, what, and how security and assurance solutions strengthen a cloud computing environment.

— *When* focuses on the timeframe in which a given solution has been proposed.
— *Where* relates to the attack surface that is the target of a given security and assurance solution.
— *What* refers to the property a given security and assurance solution considers.
— *How* considers the way in which a given solution increases security and assurance of the cloud, or in other words by which mechanisms a given security property is supported.

As an example, let us consider an approach published in May 2014 and aimed to strengthen security of data storage using a specific cryptosystem. According to our four dimensions the considered approach can be described as follows.

— *When:* May 2014.
— *Where:* tenant-on-tenant attack surface.
— *What:* integrity.
— *How:* the specific cryptosystem used to strengthen integrity of the data storage.

The above dimensions are used in Section 6.1 to provide an overview of security and assurance techniques in cloud environments.

3. VULNERABILITIES, THREATS, ATTACKS, AND RISK EVALUATION

Several works have been devoted to the evaluation of risks in the cloud, and to the identification of vulnerabilities, threats, and attacks that would target the cloud infrastructure (e.g., [Chen et al. 2008; Somorovsky et al. 2011; Cloud Security Alliance 2013; Modi et al. 2013a; Porter 2013]). Fernandes et al. [Fernandes et al. 2013] provided one of the most complete description of vulnerabilities, threats, and attacks to the cloud infrastructure. Gruschka and Jensen [Gruschka and Jensen 2010] presented a taxonomy and a classification of cloud security attacks based on the notion of attack surface. After modeling the cloud as a set of three entities including users, services, and cloud providers, they define each attack as a set of interactions within this model. First, they claim that attacks targeting the interactions between users and services are similar to the ones known for traditional distributed communications (e.g., Denial of Service – DoS, SQL injection, Cross Site Scripting – XSS). However, attacks proper of a cloud environment also involve interfaces managed by the cloud provider. Then, they identify six attack surfaces that are used, possibly in a combination, to perform an attack. Finally, they describe some successful attacks on sample cloud environments.

Here we take a similar approach to threat modeling, categorizing papers on vulnerabilities, threats, and attacks according to our broader classification of attack surface discussed in Section 2.2: *application-level*, *tenant-on-tenant*, and *provider-on-tenant*/*tenant-on-provider*. Table I shows our classification of papers discussing relevant vulnerabilities, threats, and attacks, and their mapping to attack surfaces and involved security properties.

3.1. Application-level

Application-level vulnerabilities, threats, and attacks have threatened ICT infrastructure since the early days of the Internet, and mainly target the interactions between users and services. In other words, they focus on services and data at the highest level of a cloud stack, and consider the SaaS service model. In the following, we provide an overview of vulnerabilities, threats, and attacks that focus on the cloud and its peculiarities.

Gruschka and Iacono [Gruschka and Iacono 2009] present a weakness in the SOAP-based control service of Amazon EC2 against signature wrapping attacks, originally described in [McIntosh and Austel 2005]. The attacker was able to modify an eaves-

Table I. Vulnerabilities, threats, and attacks classification based on attack surfaces and target security properties

Attack surface	Property	References
Application-level	*Confidentiality*	[Bugiel et al. 2011][Fernandes et al. 2013][Grobauer et al. 2011][Gruschka and Jensen 2010][Jensen et al. 2009] [Paquette et al. 2010][Saripalli and Walters 2010][Somorovsky et al. 2011]
	Integrity	[Booth et al. 2013][Bugiel et al. 2011][Fernandes et al. 2013][Grobauer et al. 2011][Gruschka and Jensen 2010] [Gruschka and Iacono 2009][Jensen et al. 2009][Paquette et al. 2010][Saripalli and Walters 2010]
	Availability	[Booth et al. 2013][Chonka et al. 2011][Fernandes et al. 2013][Grobauer et al. 2011][Gruschka and Jensen 2010] [Jensen et al. 2009][Liu 2010][Paquette et al. 2010][Saripalli and Walters 2010]
	Authenticity	[Fernandes et al. 2013][Grobauer et al. 2011][Gruschka and Jensen 2010][Jensen et al. 2009][Paquette et al. 2010] [Somorovsky et al. 2011]
	Privacy	[Bugiel et al. 2011][Fernandes et al. 2013][Paquette et al. 2010]
Tenant-on-tenant	*Confidentiality*	[Aviram et al. 2010][Bleikertz et al. 2013][Booth et al. 2013][Dahbur et al. 2011][Fernandes et al. 2013] [Godfrey and Zulkernine 2013][Green 2013][Grobauer et al. 2011][Gruschka and Jensen 2010] [Okamura and Oyama 2010][Paquette et al. 2010][Pearce et al. 2013][Ristenpart et al. 2009] [Saripalli and Walters 2010][Tsai et al. 2012][Zhang et al. 2012]
	Integrity	[Booth et al. 2013][Dahbur et al. 2011][Fernandes et al. 2013][Grobauer et al. 2011][Gruschka and Jensen 2010] [Paquette et al. 2010][Pearce et al. 2013][Saripalli and Walters 2010][Tsai et al. 2012]
	Availability	[Booth et al. 2013][Chonka et al. 2011][Dahbur et al. 2011][Fernandes et al. 2013][Gruschka and Jensen 2010] [Paquette et al. 2010][Pearce et al. 2013][Saripalli and Walters 2010][Tsai et al. 2012]
	Authenticity	[Dahbur et al. 2011][Fernandes et al. 2013][Gruschka and Jensen 2010][Paquette et al. 2010][Pearce et al. 2013]
	Privacy	[Aviram et al. 2010][Bleikertz et al. 2013][Dahbur et al. 2011][Fernandes et al. 2013][Okamura and Oyama 2010] [Paquette et al. 2010]
Provider-on-tenant Tenant-on-provider	*Confidentiality*	[Bleikertz et al. 2013][Booth et al. 2013][Dahbur et al. 2011][Fernandes et al. 2013][Gruschka and Jensen 2010] [Paquette et al. 2010][Rocha and Correia 2011]
	Integrity	[Fernandes et al. 2013][Gruschka and Jensen 2010][Paquette et al. 2010]
	Availability	[Dahbur et al. 2011][Fernandes et al. 2013][Gruschka and Jensen 2010][Liu 2010][Paquette et al. 2010]
	Authenticity	[Fernandes et al. 2013][Paquette et al. 2010]
	Privacy	[Bleikertz et al. 2013][Booth et al. 2013][Fernandes et al. 2013][Gruschka and Jensen 2010][Paquette et al. 2010]

dropped message faking the digital signature checking algorithm, and executed commands on behalf of legitimate users. Jensen et al. [Jensen et al. 2009] present security issues in cloud computing, considering XML signature, browser security, cloud integrity, and flooding attacks. They also introduce the cloud malware injection attack, where a malicious user tries to add a malicious service implementation and confuse the cloud provider by letting it consider the malicious service as a normal one. Somorovsky et al. [Somorovsky et al. 2011] test the security of the cloud control interfaces of Amazon public cloud and of a private cloud based on Eucalyptus. The results show that in both cases the control interfaces can be compromised by means of signature wrapping attacks. The authors propose a novel methodology for the analysis of public cloud interfaces and discuss possible countermeasures to the identified attacks. Chonka et al. [Chonka et al. 2011] focus on two attacks that can target the cloud, namely *HTTP Denial of Service* and *XML-based Denial of Service* [Srivatsa and Iyengar 2011]. In particular, they recreate the above attacks, present a solution to identify the source of an attack, and introduce an approach (*Cloud Protector*) to detect and filter these attacks. In principle, this kind of attacks could also apply to tenant-on-tenant attack surface. Bugiel et al. [Bugiel et al. 2011] provide an analysis of threats to confidentiality and privacy in the cloud that successfully extract sensitive information from Amazon machine images and exploit SSH vulnerabilities.

3.2. Tenant-on-Tenant

Tenant-on-tenant vulnerabilities, threats, and attacks are typical of virtualized environments where different tenants share a common infrastructure and may reside on the same physical hardware. Researchers working in this area mainly considered scenarios where a malicious tenant tries to attack other tenants co-located on the same hardware, exploiting misconfiguration and vulnerabilities on the virtualization infrastructure (e.g., Virtual Machine – VM – isolation). In other words, tenant-on-tenant vulnerabilities, threats, and attacks focus on resources, processes, and data at the lowest levels of a cloud stack, and consider the Paas and IaaS service models. Next, we provide an overview of papers that focus on tenant-on-tenant attack surface.

Ristenpart et al. [Ristenpart et al. 2009] describe an attack to information confidentiality of running service instances. Their attack is based on the fact that an attacker virtual machine and the target service are on the same hardware, and therefore the former can launch an attack by generating traffic and monitoring its own (or the hypervisors) performance. Aviram et al. [Aviram et al. 2010] discuss the problem of timing

channels in the cloud and present an approach to prevent timing attacks based on provider-enforced deterministic execution, while Okamura and Oyama [Okamura and Oyama 2010] consider the threat of CPU-based covert channels [Desmedt 2011] between virtual machines on the Xen hypervisor. Zhang et al. [Zhang et al. 2012] present a side-channel attack [Caddy 2011] allowing malicious virtual machines to steal private information of a target virtual machine running on the same virtual network based on Xen hypervisor. Tsai et al. [Tsai et al. 2012] study the impact of virtualization attacks on different cloud service models, while Pearce et al. [Pearce et al. 2013] discuss concerns due to inter-tenant interference in a virtualized environment. Godfrey and Zulkernine [Godfrey and Zulkernine 2013] first analyze the status of side-channel vulnerabilities involving the CPU cache, then identify drawbacks of existing defenses when applied in the cloud, and finally present a server-side solution to side-channel attack mitigation in the cloud. Green [Green 2013] presents an overview with practical examples of side-channel attacks in the cloud, allowing a malicious VM to steal sensitive information on a target VM.

3.3. Provider-on-Tenant and Tenant-on-Provider

Provider-on-tenant and tenant-on-provider vulnerabilities, threats, and attacks are specific of the cloud where users, enterprises, and business owners move their assets to an untrusted infrastructure. Researchers working in this area mainly considered scenarios where the cloud provider is malicious (or at least honest but curious) and attacks its tenants (*provider-on-tenant*). Alternatively, they consider contexts in which one or more compromised tenants (e.g., botnets for denial of service attacks) are used to attack the cloud infrastructure (*tenant-on-provider*). In other words, provider-on-tenant and tenant-on-provider vulnerabilities, threats, and attacks focus on resources, processes, and data delivered using the IaaS service model. In the following, we provide an overview of papers that focus on provider-on-tenant and tenant-on-provider attack surface.

Liu [Liu 2010] introduces a new form of denial-of-service attack, which targets and saturates the virtual network bandwidth. Clearly, this kind of attack can also be launched on application-level attack surface, where the target of the attack is a given application on a given machine. Rocha and Correia [Rocha and Correia 2011] present an overview of threats to cloud confidentiality brought by malicious insiders (which can include the cloud provider), discuss possible protection mechanisms, and describe their limitations. Bleikertz et al. [Bleikertz et al. 2013] focus on the problem of protecting a customer from attacks brought by cloud providers, also considering the scenario including malicious outsiders (tenant-on-tenant attack surface). In particular, they consider the problem of securing cryptographic operations because, in principle, providers can access stored keys and consumers are not allowed to deploy their keys at runtime only. The authors then define an architecture implementing a client-driven *Cryptography-as-a-Service* (CaaS). CaaS provides an execution domain for the client, where all encryption operations are secured and managed. It extends Xen Hypervisor and relies on trusted computing solutions.

3.4. Discussion

This section surveyed a number of research works on vulnerabilities, threats, and attacks distinguishing them on the basis of the targeted attack surfaces in the taxonomy in Figure 1. Other vulnerabilities, threats, and attacks are presented in the papers reviewed in Section 4, although their main goal is to define new approaches to strengthen cloud security.

Table I presents our main findings, including also papers reviewed in Appendix A.1. First of all, we note that surveyed papers mainly focus on application-level and tenant-

Table II. Cloud security solution classification on the basis of implemented techniques and target security properties

Security technique	Property	References
Encryption	*Confidentiality*	[Ahmed et al. 2012][Bennani et al. 2010][Bernsmed et al. 2012][Bowers et al. 2009][Chu et al. 2014] [De Capitani di Vimercati et al. 2013][De Capitani di Vimercati et al. 2014][Dsouza et al. 2013][Jajodia et al. 2013] [Juels and Oprea 2013][Kaaniche et al. 2013][Li et al. 2011b][Lin and Tzeng 2012][Pearson et al. 2009][Pattuk et al. 2013] [Peterson 2010][Sedayao et al. 2009][Thebeau II et al. 2014][Tysowski and Hasan 2013][van Dijk et al. 2012] [Zissis and Lekkas 2012]
	Integrity	[Ahmed et al. 2012][Bernsmed et al. 2012][Bowers et al. 2009][Dsouza et al. 2013][Juels and Oprea 2013][Li et al. 2011b] [Lin and Tzeng 2012][Park et al. 2013][Peterson 2010][Thebeau II et al. 2014][Wei and Reiter 2012][Wei and Reiter 2013] [Zissis and Lekkas 2012]
	Availability	[Ahmed et al. 2012][Bowers et al. 2009][Dsouza et al. 2013][Juels and Oprea 2013][Lin and Tzeng 2012] [Thebeau II et al. 2014]
	Authenticity	[Chu et al. 2014][Wei and Reiter 2013][Zissis and Lekkas 2012]
	Privacy	[Diallo et al. 2012][Jajodia et al. 2013][Kaaniche et al. 2013][Pearson et al. 2009][Pattuk et al. 2013] [Tysowski and Hasan 2013][Wang et al. 2012][Wei and Reiter 2012][Wei and Reiter 2013][Yu et al. 2013a]
Signature	*Confidentiality*	[Chow et al. 2012]
	Integrity	[Attasena et al. 2013][Shraer et al. 2010][Wang et al. 2013a]
	Availability	[Attasena et al. 2013]
	Authenticity	[Chow et al. 2012][Wei et al. 2014][Xu et al. 2013a]
	Privacy	[Attasena et al. 2013][Chow et al. 2012][Wang et al. 2013a][Wei et al. 2014]
Access control	*Confidentiality*	[Bacon et al. 2014][Barsoum and Hasan 2013][Birgisson et al. 2014][De Capitani di Vimercati et al. 2014][Kurmus et al. 2011] [Lang 2010][Li et al. 2011b][Liu et al. 2013][Nabeel et al. 2013][Okuhara et al. 2010][Peterson 2010][Singhal et al. 2013] [Takabi and Joshi 2012][Takabi et al. 2010a][Tang et al. 2012][Wan et al. 2012][Yang et al. 2013][Yu et al. 2010b][Zhu et al. 2012]
	Integrity	[Bleikertz et al. 2012][Barsoum and Hasan 2013][Kurmus et al. 2011][Lombardi and Di Pietro 2010][Lombardi and Di Pietro 2011]
	Availability	[Kurmus et al. 2011]
	Authenticity	[Barsoum and Hasan 2013][Liu et al. 2013][Nabeel et al. 2013][Ruj et al. 2014][Tang et al. 2012][Wan et al. 2012][Yang et al. 2013]
	Privacy	[Birgisson et al. 2014][Bleikertz et al. 2012][Jung et al. 2013][Raykova et al. 2012][Ruj et al. 2014][Takabi et al. 2010a] [Yu et al. 2010b][Zhu et al. 2012]
Authentication	*Confidentiality*	[Li et al. 2011a][Qin et al. 2013]
	Integrity	[Hao et al. 2011][Stefanov et al. 2012]
	Availability	[Stefanov et al. 2012]
	Authenticity	[Almulla and Yeun 2010][Ghazizadeh et al. 2012][Hao et al. 2011][Li et al. 2011a][Okuhara et al. 2010][Peterson 2010] [Qin et al. 2013][Song et al. 2009][Stefanov et al. 2012][Takabi et al. 2010a]
	Privacy	[Khalid et al. 2013]
Trusted computing	*Confidentiality*	[Bernsmed et al. 2012][Boampong and Wahsheh 2012][Krautheim 2009][Ma et al. 2013][Santos et al. 2012][Singhal et al. 2013] [Szefer and Lee 2014]
	Integrity	[Bernsmed et al. 2012][Boampong and Wahsheh 2012][Krautheim 2009][Santos et al. 2012][Singhal et al. 2013] [Szefer and Lee 2014][Velten and Stumpf 2013]
	Availability	[Ma et al. 2013]
	Authenticity	[Boampong and Wahsheh 2012]
	Privacy	[Li et al. 2013]
IDS/IPS	*Confidentiality*	[Ficco et al. 2013][Luo et al. 2014][Modi et al. 2013b][Patel et al. 2013][Stolfo et al. 2012][Xing et al. 2013]
	Integrity	[Christodorescu et al. 2009][Ficco et al. 2013][Luo et al. 2014][Modi et al. 2013b][Patel et al. 2013][Xing et al. 2013]
	Availability	[Ficco et al. 2013][Modi et al. 2013b][Patel et al. 2013][Xing et al. 2013][Yu et al. 2013b]
	Authenticity	[Lee et al. 2011]
	Privacy	[Benali et al. 2010][Stolfo et al. 2012]

on-tenant attack surfaces. This is due to the fact that, on one side, application-level attack surface has been considered since the introduction of the Internet and therefore corresponding vulnerabilities, threats, and attacks have been attempted since the cloud was first introduced; on the other side, tenant-on-tenant attack surface has been considered in several works aimed to secure virtualized environments, which can be considered as the predecessors of current cloud systems. The provider-on-tenant and tenant-on-provider attack surface is specific to the cloud and therefore less explored, although the interest on it is growing in the context of attacks to confidentiality and privacy of customer data, and availability of cloud infrastructures.

4. CLOUD SECURITY

Cloud security problems are very challenging, due to *i)* the heterogeneity of cloud stacks, *ii)* lack of formal and semantically equivalent security requirements (which often vary depending on the considered domain), *iii)* lack of a stable categorization of techniques, *iv)* need of balancing between security, flexibility, and high performance, and *v)* lack of transparency on activities and events happening in the cloud back-end. Many research works present partial, ad hoc solutions, each targeting a small part of the problem. This situation makes a general evaluation of the state of the art on cloud security difficult. Further complicating factors include potential interference between security mechanisms at different levels of the cloud stack.

In this section we present an overview of cloud security solutions. We have classified cloud security approaches according to the taxonomy of security techniques discussed in Section 2.2 (see Figure 1): encryption, signature, access control, IDS/IPS, authentication, trusted computing. Table II shows our classification together with a mapping between security solutions and supported security properties.

4.1. Encryption

The first line of research relies on encryption techniques to increase cloud security by protecting data, communication, and activities in the cloud from adversaries who aim to disrupt the cloud's normal operation, reducing the availability of cloud services, and/or inferring/accessing secret data of cloud tenants and their activities.

Most papers proposed encryption techniques to primarily achieve confidentiality, while also targeting additional properties like integrity, availability, authenticity and privacy. In 2009, Bowers et al. [Bowers et al. 2009] presented *High-Availability and Integrity Layer* (HAIL), a system that supports data file integrity and availability across different servers or independent storage services. HAIL uses a proof-of-retrievability approach to test remote storage servers and replace them if failures are detected. In the same year, Pearson et al. [Pearson et al. 2009] described different possible privacy architectures, and proposed a privacy manager component to increase the protection of private data using encryption-based obfuscation. They also provided a sample application aimed to protect metadata of shared photos. Still in 2009, Sedayao et al. [Sedayao et al. 2009] focused on protecting the confidentiality of data at rest against other users of the same storage and the system administrator. The solution they proposed is based on public key encryption and on the protection of private keys used to encrypt data. Later, in 2012, Ahmed et al. [Ahmed et al. 2012] designed a secure storage based on Reed-Solomon code to support not only data security and integrity but also availability and fault-tolerance, while Lin and Tzeng [Lin and Tzeng 2012] introduced a combination of proxy re-encryption and decentralized erasure code to form a secure storage that provides confidentiality, privacy and availability. Van Dick et al. [van Dijk et al. 2012] present the *hourglass protocol*, which provides a cryptographic approach to securely store data at rest, allows users to verify the status of their data (proving the correctness of file encryption), and increases the trustworthiness of the cloud in data management. Hourglass poses economical disincentives (significant resource constraints) to cloud providers that aim to store data in clear and at the same time pass the verification process (i.e., apply hourglass encoding on demand). Zissis and Lekkas [Zissis and Lekkas 2012] present an approach based on a Trusted Third Party (TTP) to secure user applications. The TTP is responsible for securely setting up a trust mesh between entities composing cloud constellations. The third party is used to guarantee the confidentiality, integrity, and authenticity of shared information and messages. In 2013, De Capitani di Vimercati et al. [De Capitani di Vimercati et al. 2013] proposed a solution to assess the integrity of the results of join queries. Their approach considers a honest-but-curious storage server and malicious external computational providers, which produce the join results calculated over externally stored databases. Jajodia et al. [Jajodia et al. 2013] consider the problem of how to securely backup encryption keys for *i)* increasing data safety and availability, *ii)* reducing the risk of data loss due to unavailability of keys, and *iii)* limiting the risk of key disclosure and confidentiality breach. The authors present a scheme called *recoverable encryption through a noised secret* that allows to store key backups on a single machine, and is robust to decryption by brute force attacks. Decryption is in fact computationally intensive and time consuming. Juels and Oprea [Juels and Oprea 2013] focus on the migration of enterprise data to the public cloud, while maintaining a level of trust and visibility on the correctness of tenant operations. Their approach is based on cryptographic protocols and aims to provide strong protection on migrated data. It relies on an auditing framework to verify internal properties of the cloud and provide the desired level of assurance that enterprise data are managed to preserve security and reliability. Kaaniche et al. [Kaaniche et al. 2013] introduce a solution based on ID-Cryptography [Libert and Quisquater 2011] to protect the confidentiality of data in cloud-based storage. Also,

it offers a set of functionalities supporting controlled access to data and preventing unauthorized access against untrusted parties. Bennani et al. [Bennani et al. 2010] provide a solution based on homomorphic variation of a joint encryption technique providing simple key management and revocation schemes for the cloud. Their solution is based on virtual role keys implemented as a set of shares distributed between different servers, which are then used to enforce access policies of data owners and collaboratively execute encrypted queries of users. Pattuk et al. [Pattuk et al. 2013] describe a framework called *BigSecret* for secure outsourcing and protection of encrypted data over key-value stores. BigSecret provides three encryption models at the basis of the approach supporting *i)* secure data management on semi-trusted providers and *ii)* queries on encrypted data. The models use crypto indices, based on bucketization or pseudo random functions, and allow delete, get, and scan operations over encrypted data. BigSecret also provides a heuristic supporting secure distribution of data and workloads to increase performance and efficiency. It considers a cloud scenario consisting of multiple providers with monetary and disclosure risk constraints. Tysowski and Hasan [Tysowski and Hasan 2013] propose a protocol for secure outsourcing of data to the cloud. The protocol, relying on an attribute-based encryption scheme, a group keying mechanism, and re-encryption, protects data against the cloud provider. It supports revocation and allows users with the right attributes to access data. The protocol is also designed to support resource-constrained mobile devices, delegating computation to the cloud provider/third parties. Recently, Chu et al. [Chu et al. 2014] designed a key-aggregate cryptosystem that allows to aggregate secret keys compacting them into a single key. The resulting key includes the power of all the aggregated keys.

Encryption techniques have been also used to exclusively ensure properties different than confidentiality. Diallo et al. [Diallo et al. 2012] present a middleware, called CloudProtect, which provides encryption functionalities for protecting data privacy in the cloud. CloudProtect implements a set of functionalities transparent to applications that allow to store encrypted data on the service provider and operate directly on them whenever possible. In case plaintext data are necessary, CloudProtect implements a protocol exposing them for a limited amount of time. Wang et al. [Wang et al. 2012] and Yu et al. [Yu et al. 2013a] introduce solutions supporting secure search, in particular ranked keyword search and multikeyword top-k search, over encrypted storage. Wei and Reiter [Wei and Reiter 2013] present a protocol that allows pattern-matching applications to access data also in encrypted form. Their approach is based on the evaluation of a deterministic file automaton on an encrypted file stored in the cloud. The paper builds on the work in [Wei and Reiter 2012] and extends it by permitting the client to identify any cloud provider misbehavior. Park et al. [Park et al. 2013] present THEMIS, a security-enhanced system for billing supervision. The proposed approach provides mutually verifiable binding information for dispute resolution and a monitoring-based approach for SLA verification based on a trusted platform.

4.2. Signature

Some approaches use encryption-based digital signatures to support integrity, privacy, or both properties. In particular, Shraer et al. [Shraer et al. 2010] present *Venus*, a service that makes the interactions of users with untrusted cloud storage more secure. Venus ensures integrity and consistency for applications via a key-based object store service that does not require trusted components or changes to the storage provider. Attasena et al. [Attasena et al. 2013] introduce a multi-secret sharing scheme based on block cryptography, secret sharing, and hash functions in which two types of signatures are employed to support data availability and integrity. The first one is an inner signature created from all data in each shared data block, which is used to verify data integrity. The second one is an outer signature created from each encrypted data

block, which allows to quickly identify and correct erroneous data blocks and preserve data availability. Wang et al. [Wang et al. 2013a] define a solution based on a security mediator implementing an anonymous approach to cloud data integrity verification. Verification metadata based on signatures are used to provide anonymous proofs of data possession. In addition, the security mediator does not learn information about data uploaded to the cloud. While the three previous works focus on integrity, Chow et al. [Chow et al. 2012] introduce a solution for data sharing that uses verifier-local revocable group signature and identity-based broadcast encryption to provide confidentiality, anonymity, and traceability properties. The key idea in this solution is the design of a group signature that is not only verifier-local revocable but also traceable and exculpable. Wei et al. [Wei et al. 2014] propose an auditing protocol for discouraging privacy cheating. Their proposal relies on batch verification as well as on ad hoc probabilistic sampling mechanisms. A work based on signatures that does not target integrity and privacy is the one by Xu et al. [Xu et al. 2013a]. The authors introduce *Software Service Signature* (S3), a solution that aims to address free-riding issues of SaaS, where malicious participants may try to maximize their benefits in using the service. The basic idea of S3 is to increase security through authentication via ID-based proxy signature from pairings [Libert and Quisquater 2011], so that service requests are always verifiable.

4.3. Access control

Existing access control systems for distributed environments are not directly applicable to the cloud. As a consequence, the research community has defined new approaches to access control in the cloud. We review them in this section, together with security solutions which *i)* implement authorization mechanisms, and *ii)* use monitoring approaches to distinguish between benign and malicious accesses to cloud resources.

In 2010, Lang et al. [Lang 2010] presented a solution to security and compliance policy automation and configuration. They supported the generation of technical policies according to a model-driven transformation. Also, they provided an approach to incident reporting and management of application authorizations. An implementation based on *OpenPMF*, a fully-fledged model-driven security product, is provided supporting modeling, auto-generation, enforcement, monitoring, and automatic update of policies. In the same year, Yu et al. [Yu et al. 2010b] employed a combination of attribute-based encryption, and proxy and lazy re-encryption. The result is a fine-grained, scalable technique for cloud access control. Still in 2010, Lombardi and Di Pietro [Lombardi and Di Pietro 2010] presented a system called *Transparent Cloud Protection System* (TCPS), protecting cloud security and transparently monitoring the integrity of cloud components. Later, Lombardi and Di Pietro developed their approach to propose *Advanced Cloud Protection System* (ACPS) [Lombardi and Di Pietro 2011], an architecture protecting integrity of guest VMs and other infrastructure components. The architecture takes advantage from cloud virtualization, can be deployed on different cloud stacks, and monitors the integrity of all involved components. Kurmus et al. [Kurmus et al. 2011] present two architectures aimed to achieve efficient security of the storage service in a multi-tenant scenario as follows: *i)* the first isolates customers in VMs at hypervisor level, *ii)* the second uses mandatory access control in a shared/centralized OS kernel. The period of 2012–2013 was one of intense research on cloud access control. Tang et al. [Tang et al. 2012] present a policy-based access control relying on selective encryption with assured file deletion. Their approach employs a set of encryption operations that are maintained by a set of independent key managers, whose number is above a given threshold. Zhu et al. [Zhu et al. 2012] provide a temporal access control approach for the cloud, which associates an access policy on tem-

poral attributes to each outsourced resource. In their approach, proxy re-encryption is used to match access policies and user's attributes in the access request. Takabi and Joshi [Takabi and Joshi 2012] describe *Policy Management as a Service* (PMaaS), a unified framework for policy management in the cloud. PMaaS provides a single control point that is independent from resource location. In order to prevent insider attacks, Bleikertz et al. [Bleikertz et al. 2012] introduce an approach to perform cloud maintenance, protecting privacy and integrity of users' workloads with respect to system administrators. Their approach is based on five fine-grained privilege levels. Raykova et al. [Raykova et al. 2012] propose a solution aimed to protect private information in access control policies as well as users' access patterns from the prying eyes of the cloud provider. The authors define an access control system working at two levels: *i)* cloud-side, using a coarse-grained access control to limit the amount of information accessible to the cloud provider, *ii)* client-side, using fine-grained selective encryption access control to guarantee a proper level of expressiveness. The idea of extending *Ciphertext-Policy Attribute-Based Encryption* (CP-ABE) for supporting fine-grained access control schemes is exploited in three different papers: the ones by Wan et al. [Wan et al. 2012], Liu et al. [Liu et al. 2013] and Yang et al. [Yang et al. 2013]. CP-ABE is a possible approach to attribute-based encryption where, differently from traditional encryption, ciphertexts and users' decryption keys correspond to an attribute set or an attribute-based policy [Wan et al. 2012]. In particular, CP-ABE encrypts the ciphertext with a tree access policy. The associated decryption key is generated according to a set of attributes. The user can use the decryption key to access the ciphertext if the set of attributes referring to the key satisfies the tree access policy of the ciphertext. Wan et al. [Wan et al. 2012] propose a *Hierarchical Attribute-Set-Based Encryption* (HASBE) access control scheme with users organized in a a hierarchical structure. Liu et al. [Liu et al. 2013] introduce another fine-grained access control scheme with authentication, a hierarchy of multi-authorities, and attribute-based signature. Yang et al. [Yang et al. 2013] design *Data Access Control for Multi-Authority Cloud Storage* (DAC-MACS). DAC-MACS is an encryption-based access control scheme, which supports revocation. Key management is performed by multiple authorities, addressing forward and backward security. Nabeel et al. [Nabeel et al. 2013] propose an attribute-based access control for file sharing based on a new key management scheme that is able to add/revoke users or update attribute-based access control policies simply by modifying some public information. Barsoum and Hasan [Barsoum and Hasan 2013] design a solution that not only provides confidentiality, integrity, and authorization for data, but also efficiently controls versions of data and supports symmetric chain of trust between the data owner and the cloud provider. A different approach is taken by Jung et al. [Jung et al. 2013] to design *AnonyControl*, an anonymous attribute-based privilege control scheme that exploits multiple authorities to protect user privacy in a cloud storage server. AnonyControl provides both fine-grained privilege control and anonymity. Recently, Bacon et al. [Bacon et al. 2014] evaluated the suitability of *Information Flow Control* (IFC), a mandatory access control approach, to secure cloud infrastructures. They presented different *IFC* and *Decentralised IFC* (DIFC) solutions, mainly focused on PaaS level (claimed as the most appropriate model for DIFC integration), and evaluated issues and challenges of adopting IFC and DIFC in cloud scenarios. Ruj et al. [Ruj et al. 2014] present a decentralized access control scheme for secure data storage in clouds that is able to verify the authenticity of the submitted information without the need of knowing user identity, while Birgisson et al. [Birgisson et al. 2014] introduce authorization credentials (called *macaroons*) for cloud services supporting decentralized delegation based on nested and chained Message Authentication Codes (MACs) [Preneel 2011].

4.4. Authentication

Some work has also been done on adding authentication and identity management to the cloud.

In 2009, Song et al. [Song et al. 2009] presented *TrustCube*, an approach supporting the management of authentication in the cloud for mobile users. TrustCube provides an independent, policy-based platform for cloud authentication, integrating a number of authentication techniques. A year later, in 2010, Almulla and Yeun [Almulla and Yeun 2010] presented an overview of security and privacy issues in the cloud, focusing on Identity and Access Management (IAM), IAM lifecycle, and IAM standards and protocols (e.g., Security assertion Markup Language – SAML, Open Authentication – OAuth – protocol). Then, in 2011, Hao et al. [Hao et al. 2011] designed a time-bound ticket-based scheme for mutual authentication between the cloud and users, which incorporates a service for data integrity verification without access to stored data. Li et al. [Li et al. 2011a] propose the design of a hierarchical architecture for cloud computing that employs identity-based cryptography to support both data confidentiality and user authentication. Ghazizadeh et al. [Ghazizadeh et al. 2012] analyze security issues that could affect federated identity and single sign-on in the cloud, and present some models that could be used to counteract identity theft in federated environments. Stefanov et al. [Stefanov et al. 2012] propose the use of Merkle trees [Carminati 2009] to provide authentication for *IRIS*, an authenticated cloud-based file system. In IRIS, a Merkle tree consists of three main components: block-level MAC, file version tree, and directory tree. Based on the Merkle tree, IRIS is able to support both authentication and data integrity verification. Besides, IRIS also supports data availability via a proof-of-retrievability protocol that can quickly identify corrupted or inaccessible data pieces for data recovery. Khalid et al. [Khalid et al. 2013] introduce an authentication and authorization protocol that smoothly integrates with an IDentity Management System (IDMS) to preserve the privacy of users. In their approach, anonymity is provided in the authentication and authorization protocol by replacing real identities of users with anonymous identities and keys generated and managed by the IDMS. On the other hand, Qin et al. [Qin et al. 2013] present a general framework providing simultaneous authentication and secrecy for data upload, based on an identity-based "signcryption" scheme that can perform encryption and signature at the same time.

4.5. Trusted computing

Trusted computing relies on *Trusted Platform Modules* (TPMs) [Morris 2011] and related hardware to prove integrity of software, processes, and data. The advent of the cloud, however, requires to adapt hardware TPM to virtualized environments.

A seminal paper is the one by Krautheim [Krautheim 2009], which defines a private virtual infrastructure for the cloud sharing responsibility between users and providers, and decreasing the overall risk of exposure. The proposed approach is based on the notion of *virtual Trusted Platform Module* (vTPM), introduced in [Berger et al. 2006], which provides secure storage and cryptographic functions of TPM to applications and operating systems running in virtual machines. vTPM is composed of *vTPM instances*, each associated with a virtual machine that needs TPM functionalities, and a *vTPM manager* that instantiates vTPMs and multiplexes requests coming from virtual machines. Boampong and Wahsheh [Boampong and Wahsheh 2012] later gave an overview of cloud security focusing on data storage security, cloud security risks, security policies, physical security, and cloud software security. The authors claim that authentication, confidentiality, and integrity properties can be achieved by enriching cloud with a trusted computing platform. Following the work of Boampong and Wahsheh, Santos et al. [Santos et al. 2012] introduce *Excalibur*, a system that provides

data confidentiality and integrity by encrypting data according to a customer-defined policy and guaranteeing that data are only decrypted by nodes whose configuration matches the policy. Ma et al. [Ma et al. 2013] employ trusted computing to address the security issues of virtual machine replication, which is triggered to improve the availability of data and services in the cloud.

Not all trusted computing techniques applicable to the cloud are encryption-based. Li et al. [Li et al. 2013] present *MyCloud*, an architecture for privacy protection that departs from traditional encryption mechanisms. MyCloud reduces as much as possible the trusted computing base (e.g., putting the control of VMs out of its scope) and permits clients to configure their privacy protection, reducing at the same time the ability of the cloud provider of modifying privacy settings. Departing from vTPM, Velten and Stumpf [Velten and Stumpf 2013] provide a solution proving integrity of several different virtual machines using a single hardware TPM. The presented approach does not allow an attacker to tamper with the mapping between a VM and each integrity measurement, and stores the latter in a concealed manner to prevent information leakage by other tenants during remote attestation. Recently, Szefer and Lee [Szefer and Lee 2014] proposed a secure hardware infrastructure increasing the protection of users' code and data, against attacks from other tenants and malicious software in the cloud.

4.6. IDS/IPS

The availability of computational resources as commodities on demand, makes the cloud a powerful weapon in the hands of malicious users, who can use cloud resources for attacks (e.g., Distributed Denial of Service – DDoS), and a tool in the hands of security experts, who can use cloud resources to deploy IDS and IPS. Recently, Modi et al. [Modi et al. 2013b] surveyed different attacks affecting availability, confidentiality, and integrity, and reviewed approaches providing IDS and IPS in the cloud. The authors focus on insider attacks, flooding attacks, user to root attacks, port scanning, attacks on hypervisor or VMs, and backdoor channel attacks. Then they present the evolution of IDS and IPS, and explain how IDS and IPS have been used to increase cloud security. The authors also present a useful summary of existing IDS approaches (see Table 4 in [Modi et al. 2013b]) discussing their advantages and drawbacks. Patel et al. [Patel et al. 2013] investigate new issues, challenges, and requirements when intrusion detection and prevention functionalities are deployed in the cloud and introduce a survey of existing technologies, while Ficco et al. [Ficco et al. 2013] provide a survey of cloud-oriented distributed intrusion detection systems. The latter survey presents a distributed, hierarchical, and multi-layer architecture for intrusion detection, which supports complex event correlation analysis.

Some approaches to intrusion detection and prevention in the cloud are summarized below. With respect to traditional IDS, Christodorescu et al. [Christodorescu et al. 2009] consider an important aspect in cloud security, namely, the security of VMs over which cloud services and functionalities are deployed. They propose an approach to increase VM introspection [Ardagna et al. 2014] and provide an architecture securing the customers' virtualized workloads. The approach makes no assumption on the integrity of the VMs. The paper also describes a rootkit-detection and rootkit-recovery service running outside the VM as an application of the presented introspection approach. Lee et al. [Lee et al. 2011] propose a multi-level intrusion detection system that checks the users' authentication information and applies different levels of security strength to them based on their degree of anomaly. The anomaly level of users is determined based on their configuration (such as the IP coverage and vulnerable ports) and then updated regularly based on their behavior in using the cloud. Benali et al. [Benali et al. 2010] present a distributed and privacy-preserving network intru-

sion detection system. Their approach is based on collaborative intrusion detection and on secure multiparty computation for privacy-enhanced evaluation of the global state of the network.

Considering IPS, Stolfo et al. [Stolfo et al. 2012] present *fog computing*, a solution to mitigate data theft attacks from insiders in the cloud. Their proposal is based on decoy technology that launches a disinformation attack when an insider attack is detected through monitoring. Yu et al. [Yu et al. 2013b] define a resource allocation solution based on intrusion prevention servers, which permits to counteract DDoS attacks. The proposed solution focuses on protecting servers that are vulnerable to DDoS attacks; to this aim, it employs different intrusion prevention servers to distinguish malicious from normal traffic directed to the entity under attack. Variable attack surfaces have also been used as an attack mitigation strategy. Xing et al. [Xing et al. 2013] present *SnortFlow*, an open-flow intrusion prevention system that automatically reconfigures the cloud networking system to counteract attacks. Recently, Luo et al. [Luo et al. 2014] proposed a federated cloud security architecture that proactively defends the cloud against cyber threats and attacks, by deploying controls at application, network, and system levels.

4.7. Discussion

This section surveyed a set of papers whose main goal is to define new approaches to strengthen cloud security, against different threats, vulnerabilities, and attacks.

Table II presents our main findings, including also papers reviewed in Appendix A.2. First of all, in line with the results of previous surveys (e.g., [Iankoulova and Daneva 2012]), we found that confidentiality and integrity are still the most researched categories of properties. Most solutions focused on encryption-based techniques and access control systems. More recently, however, research on IDS/IPS and trusted computing experienced an increase, as well as research aimed to protect the privacy of cloud tenants. We also remark that, while signature techniques are often used to strengthen security, they are mostly used together with other techniques. Availability has been the target of a minor number of work, focusing on DDoS attacks. This finding is mainly due to the fact that availability is often seen as a property at the border between the security, reliability, and performance research areas. More detailed results are presented in Section 6.1.

5. CLOUD ASSURANCE

Progress in cloud security research fostered the development of assurance techniques rising the confidence of the users that a cloud stack and its services comply with their non-functional requirements. As discussed in the introduction, assurance is a much wider notion than the one of security, unanimously defined by many sources[2] as "*the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction*". Indeed, in the cloud, it is perfectly possible to have good security and poor assurance, as for instance when the operation of sound security mechanisms is not made visible to the users. Many times, however, poor assurance goes hand in hand with poor security. More importantly, poor assurance usually prevents proving that security and privacy properties of a process comply with laws and regulations.

The concept of *transparency*, that is, higher access to low-level (back-end) data produced by the cloud infrastructure and to evidence collected on the security of cloud data and applications, has been recognized as the basis for an effective approach to

[2]See for instance SP 800-37; SP 800-53; SP 800-53A; SP 800-18; SP 800- 60; CNSSI-4009; FIPS 200; FIPS 199; 44 U.S.C., Sec. 3542.

Table III. Cloud assurance solution classification on the basis of implemented assurance techniques

Assurance technique	References
Testing	[Bai et al. 2011][Bai et al. 2013][Candea et al. 2010][Chan et al. 2009][Ciortea et al. 2010][Gao et al. 2011][Gao et al. 2013] [Hanawa et al. 2010][Jayasinghe et al. 2012][King and Ganti 2010][Koeppe and Schneider 2010][Lu et al. 2014][Mahmood et al. 2012] [Moreno 2010][Parveen and Tilley 2010][Pham et al. 2011][Riungu et al. 2010][Starov and Vilkomir 2013][Tsai et al. 2011] [Yu et al. 2010a][Zech 2011]
Monitoring	[Aceto et al. 2013][Alhamazani et al. 2013][Foster and Spanoudakis 2011a][Foster and Spanoudakis 2011b][Ganglia 2014] [Kai et al. 2013][Meng and Liu 2013][Massie et al. 2012][Mohamaddiah et al. 2014][Monfared and Jaatun 2011][Nagios 2014] [Rao et al. 2013][Shao et al. 2010][Sundareswaran et al. 2012][Wang et al. 2010][Zou et al. 2013]
Certification	[Bertholon et al. 2011][Cimato et al. 2013][Grobauer et al. 2011][Khan and Malluhi 2010][Krotsiani et al. 2013] [Muñoz and Maña 2013][Spanoudakis et al. 2012][Sunyaev and Schneider 2013]
Audit/compliance	[Birnbaum et al. 2013][CSA 2014][Doelitzscher et al. 2012][Doelitzscher et al. 2013][Doelitzscher et al. 2013][Haeberlen 2010] [Mei et al. 2013][Ni et al. 2014][Pearson 2011][Rajkumar et al. 2013][Rasheed 2013][Shetty 2013][Wang et al. 2011][Wang et al. 2014] [Wang et al. 2010][Wang et al. 2013b][Wang et al. 2013][Wang et al. 2012][Yang and Jia 2013][Zawoad et al. 2013][Zhu et al. 2013]
SLA	[Anisetti et al. 2014][Bernsmed et al. 2011][Casalicchio and Silvestri 2013][CIO 2012][Garg et al. 2013][Jhawar and Piuri 2013] [Jin et al. 2013][Marinescu et al. 2013][Mouratidis et al. 2013][Sakr and Liu 2012][Sulistio and Reich 2013][Wieder et al. 2011] [Ye et al. 2012][Zhao et al. 2012]

cloud assurance [Ardagna et al. 2014; Spanoudakis et al. 2012]. Lack of transparency in fact makes the cloud and its security issues not clear to end-users. Chauhan et al. [Chauhan et al. 2013] claim that security threats "*require cloud customer to look for more transparency and controls*" and that "*SLAs and contracts do not provide technical and measurable method to find the security control status of cloud hosted application/data*". They present an approach supporting the measurement of the security status of a system. In particular, they propose a *Security Measurement System* (SMS) that interacts with cloud-hosted applications to retrieve metric information. Jenkins [Jenkins 2013] claims that there are three fundamental aspects to consider for securing businesses moving to the cloud. Firstly, there is the need of a solution to risk assessment and management, evaluating the impact a movement to the cloud would have on the business. The second aspect is transparency, meaning that the cloud customers must be well aware of cloud provider practices. Thirdly, policy and compliance become a must. Cloud providers, following the transparency requirement, should not only show their compliance to standards/regulations and the supported policies, but also explain how they achieve and maintain their compliance levels under the "comply-or-explain" principle [MacNeil and Li 2006]. In [Knode 2009], the concept of transparency is introduced as a way to document, evaluate, and observe "*technical controls (e.g., auditing, access control, system configuration, encryption), management controls (e.g., vulnerability assessments, risk assessments, system and service acquisition), and operational controls (e.g., configuration management, awareness and training, change management)*". Also, transparency aims to provide a trusted cloud service, which evaluates cloud providers and their trustworthiness. In this context, *CloudTrust Protocol* (CTP) is the mechanism under the user control allowing it to ask and retrieve information about the cloud provider infrastructure. In addition, according to [Ardagna et al. 2014], transparency is fundamental to support both *introspection*, that is, the capability of a cloud provider of examining and observing its internal processes, and *outrospection*, that is, the ability of customers and service providers to examine and observe cloud's internal processes, involving their activities, data, and applications, for security purposes. A proper solution to assurance in the cloud should embrace both introspection by cloud providers and outrospection by cloud customers (tenants in general), and therefore balance the burden of security processes and controls between providers and customers.

In this section, we survey approaches to the verification and validation of cloud infrastructures. Cloud assurance approaches have been categorized according to the classification of assurance techniques in Section 2.2: testing, monitoring, certification, audit/compliance, SLA. These categories of solutions focus on increasing trust in the cloud infrastructure, can target all levels of the cloud stack, and aim to empower cloud users. Table III shows our classification of cloud assurance solutions based on the implemented assurance techniques.

5.1. Testing

The first class of approaches to software and service validation and verification is based on testing. According to ISTQB glossary [van Veenendaal 2012], testing is "*the process consisting of all lifecycle activities, both static and dynamic, concerned with planning, preparation and evaluation of software products and related work products to determine that they satisfy specified requirements, to demonstrate that they are fit for purpose and to detect defects.*". Test-based approaches can be applied at all layers of the cloud stack and can be used to give the assurance that a certain property is held by a given cloud service/functionality [Riungu et al. 2010]. Usually, techniques for testing in the cloud can be grouped in two main categories: solutions for testing the cloud infrastructure and solutions using cloud resources to test any kind of software applications (including cloud services).

Chan et al. [Chan et al. 2009] present a modeling of the cloud as a graph and a set of model-based testing criteria. Moreno [Moreno 2010] describes a solution to the testing and benchmarking of cloud storage systems. He defines and implements a distributed testing framework, which produces different amounts of load, performs simple put/get operations, logs events and activities from the cloud storage system, and interacts with the cloud and its behavior. The framework also produces statistics which are used to outline system behavior and results of the testing activities. King and Ganti [King and Ganti 2010] introduce the first solution to move autonomic self-testing to the cloud. They combine an automated test script for cloud services with a *Test Support as-a-Service* (TSaaS), providing partial automation of testing activities of remote cloud services. Tsai et al. [Tsai et al. 2011] present a testing approach for service compositions in the cloud. Their solution is based on group testing to identify an oracle, which is then used to continuously test new services or compositions. Zech [Zech 2011] presents a model-driven methodology for cloud security testing, where tests are generated according to negative requirements that, in turn, are the outcome of risk analysis. Pham et al. [Pham et al. 2011] describe *CloudVal*, a software-implemented fault injection framework automating fault injection-based experiments. CloudVal supports reliability verification and black box testing in virtualized environments. Bai et al. [Bai et al. 2011] survey existing cloud testing tools. They consider different approaches to cloud testing such as traditional tools moved to the cloud, research and commercial tools, and specific benchmarks and testbeds. However, they do not focus specifically on cloud security. In a different survey, Gao et al. [Gao et al. 2011] provide a literature review on cloud testing and cloud-based application testing. They present a summary of issues, challenges, and problems, compare web-based software testing vs cloud-based application testing, and describe existing commercial products and solutions for cloud testing. Later, Gao et al. continued their work analyzing issues and challenges of SaaS testing [Gao et al. 2013]. Recently, Lu et al. [Lu et al. 2014] proposed a solution to service composition with global trust based on *i)* random assessments for objective Quality of Service (QoS) such as execution time, reliability, availability, throughput, and *ii)* client/service provider trust evaluation for subjective QoS.

Another line of research uses the cloud as a platform for application testing. Parveen and Tilley [Parveen and Tilley 2010] present a general discussion to establish when it is worth to move software testing to the cloud. Their evaluation considers the peculiarities of the application under evaluation and the testing activities to be performed on it. Working on a specific solution, Ciortea et al. [Ciortea et al. 2010] present *Cloud9*, an on-demand testing service that runs in the cloud. Cloud9 provides fast, complete, and automated testing of real software by means of parallel symbolic execution. Hanawa et al. [Hanawa et al. 2010] present a testing environment, called *D-Cloud*, that can be deployed in the cloud. D-Cloud is designed for dependable parallel and distributed sys-

tems. Their solution tries to address the problem of testing information systems, which are increasingly complex and distributed. Candea et al. [Candea et al. 2010] introduce the notion of *Testing-as-a-Service* (TaaS). They present a cloud-based application implementing a TaaS-automated software testing solution in three versions: *i)* "programmer's sidekick" providing developers with an environment to test their application code with little investment of resources, *ii)* "home edition" providing a testing service that supports customers in testing the software they are ready to install on local PCs or mobile devices, and *iii)* public "certification service" assessing software reliability, safety, and security. To support TaaS efficiently, Yu et al. [Yu et al. 2010a] present a solution that defines scheduling and dispatching algorithms to increase cloud computing resource utilization. In different approaches, Koeppe and Schneider [Koeppe and Schneider 2010] and Jayasinghe et al. [Jayasinghe et al. 2012] introduce solutions focusing on testing the performance of cloud services. Mahmood et al. [Mahmood et al. 2012] rely on the cloud to automatically test the security and robustness of Android apps in a scalable way. Recently, Starov and Vilkomir [Starov and Vilkomir 2013] presented *Cloud Testing of Mobile Systems* (CTOMS), an integrated TaaS solution of mobile systems with a core infrastructure that enables the scaling of additional functionalities, while Bai et al. [Bai et al. 2013] introduced the design and implementation of *Vee@Cloud*, a platform-independent virtual test lab to provide on-demand testing services and Internet-scale testing capabilities.

5.2. Monitoring

In addition to approaches for software testing in the cloud, much effort has been done on cloud software and service monitoring. In fact, cloud gives limited access to information about the status of services, as well as on events and activities happening in its back-end. Monitoring can help to increase the level of transparency in the cloud, and in turn the overall cloud security. Existing approaches to distributed system monitoring support different kinds of monitoring, ranging from monitoring of individual software services (e.g., [Mahbub and Spanoudakis 2004; Bianculli and Ghezzi 2007]), to service compositions, workflows, or orchestrations (e.g., [Baresi and Guinea 2005; Moser et al. 2008; Dranidis et al. 2009; Hallé and Villemaire 2009; Simmonds et al. 2009]), infrastructures for service-based systems (e.g., grid and cloud systems [Truong_c and Fahringer 2004; Andreozzi et al. 2005; Clayman et al. 2010; Ganglia 2014; Nagios 2014]), SLAs (e.g., [Ghezzi and Guinea 2007; Mahbub and Spanoudakis 2007]), or the context of service-based systems (e.g., [Salifu et al. 2007; Kang et al. 2008]).

Focusing on cloud environments, several general-purpose monitoring solutions can be used for cloud security monitoring. Ganglia [Massie et al. 2004; Massie et al. 2012; Ganglia 2014] and Nagios [Nagios 2014] are two widespread open source distributed monitoring systems. Ganglia [Ganglia 2014] supports performance monitoring of clusters and grids; Nagios [Nagios 2014] defines a general purpose toolkit for monitoring diverse IT infrastructure assets, including applications, network protocol drivers, operating systems, and other software components. Shao et al. [Shao et al. 2010] propose a *Runtime Model for Cloud Monitoring* (RMCM). RMCM collects raw data from several monitoring probes and presents them in a more intuitive form. The proposed approach finds a balance between monitoring overhead and capability, by managing monitoring facilities in an adaptive fashion. Wang et al. [Wang et al. 2010] define a monitoring approach that fits cloud complexity. They propose a scalable solution to perform analysis and correlation of logs for cloud hardware and software components. Their work extends the *Run-Time Correlation Engine* (RTCE) [Holub et al. 2009] to provide a scalable approach for the cloud. The SLA@SOI project developed a dynamically configurable monitoring infrastructure [Foster and Spanoudakis 2011a; 2011b]. The proposed infrastructure can automatically adapt to changes in the monitoring func-

tionalities available to service-based systems, and control and monitor SLAs, including agreements on security properties. Monfared and Jaatun [Monfared and Jaatun 2011] provide an overview of existing security monitoring mechanisms and how they can be adapted to the cloud. They analyze new issues, challenges, and requirements when moving monitoring functionalities to the cloud and propose approaches to mitigate them. Sundareswaran et al. [Sundareswaran et al. 2012] introduce a cloud information accountability framework that keeps track of user data usage in the cloud. Their approach integrates automatic data access logging and an auditing mechanism, and supports strong back-end protection. Zou et al. [Zou et al. 2013] present a trusted monitoring framework for virtualized cloud platforms. Their approach is based on an independent guest domain for monitoring and on trusted computing to guarantee framework integrity, and addresses the trust challenges between cloud providers and their tenants. Rao et al. [Rao et al. 2013] develop previous work on fuzzy service selection [Bosc et al. 2001] to propose *DynaQoS*, a self-tuning fuzzy control framework that includes "*mechanisms for self-tuning output amplification and flexible rule selection*". DynaQoS [Rao et al. 2013] supports "*adaptive multi-objective resource allocation and service differentiation*". Alhamazani et al. [Alhamazani et al. 2013] identify and discuss the major design issues related to engineering cloud monitoring tools, while Kai et al. [Kai et al. 2013] present the design of *SCM*, a monitoring system working within Apache CloudStack platform, and its main components. Aceto et al. [Aceto et al. 2013] provide a survey on cloud monitoring. The survey focuses on platforms, mechanisms, and products for cloud infrastructure, service, and application monitoring. Meng and Liu [Meng and Liu 2013] discuss the idea of *Monitoring-as-a-Service* (MaaS), and present the major components and key functional requirements of MaaS in the cloud. Mohamaddiah et al. [Mohamaddiah et al. 2014] also introduce a survey on cloud monitoring, while the main focus is on resource allocation and management.

5.3. Certification

The use of certification techniques to provide enough evidence that a software system holds some non-functional properties and behaves correctly has become widespread in the last twenty years and is also becoming important in cloud environments. Many certification solutions and schemes have been proposed in the past. A survey of certification schemes used to evaluate and certify security properties of software in general, and of security controls in particular, can be found in [Damiani et al. 2009a]. However, as pointed out in [Anisetti et al. 2013b], "*existing certification techniques are not well-suited to the service scenario*", and in turn to the cloud scenario. In fact, such techniques "*usually consider static and monolithic software, provide certificates in the form of human-readable statements, and consider system-wide certificates to be used at deployment and installation time*". By contrast, in a cloud environment, a certification scheme needs to accomplish the dynamic, multi-level, and hybrid nature of clouds. In addition, it must integrate with cloud-specific runtime processes, involving service deployment, discovery, selection, and composition, and management activities, including migration, elasticity, and resource allocation.

The first step towards cloud certification consists in the definition of certification solutions for services. Damiani et al. [Damiani et al. 2009b] study the issue of assessing and certifying SOA operation, by means of security certificates including signed test cases. Also, the US-based Software Engineering Institute (SEI) [SEI 2011] defines a certification and accreditation process for services following requirements by the US Army CIO/G-6. Kourtesis et al. [Kourtesis et al. 2010] use Stream X-machines to increase SOA reliability. Their solution manages conformance testing via the SOA registry, which evaluates functional equivalence between a service and its specifications. If equivalence is verified, a certificate is awarded to the service. Furthermore,

some papers (e.g., [Ryu et al. 2008; Papazoglou et al. 2011]) analyze the management of evolving services subject to dynamic changes. This scenario, which introduces the need of continuous service re-design, has direct impact on cloud/service security certification. Changes may in fact invalidate certificates, thus requiring re-certification. Anisetti et al. [Anisetti et al. 2012; 2013a; Anisetti et al. 2013b] propose a security certification scheme that implements a model-based testing approach, and extends it to cope with certification of evolving services and service compositions. The proposed solution relies on a Symbolic Transition System (STS)-based service modeling to the aim of automatically generating test cases for service certification.

Focusing on cloud computing, only a few preliminary solutions to the cloud certification problem have been proposed. Khan and Malluhi [Khan and Malluhi 2010] discuss the problem of establishing trust between the cloud and its customers, and describe possible approaches to support trust in the cloud, including service certification. From a different point of view, Grobauer et al. [Grobauer et al. 2011] provide an overview of current vulnerabilities affecting the cloud at different levels, and identify certification as a preferred approach for vulnerability management. Spanoudakis et al. [Spanoudakis et al. 2012] discuss the need of providing novel models for cloud service certification and present a hybrid, incremental, and multi-layer approach to cloud certification. Sunyaev and Schneider [Sunyaev and Schneider 2013] present an overview of the possible benefits a certification solution for cloud services could give to all cloud actors, addressing the lack of transparency, trust, and acceptance. Bertholon et al. [Bertholon et al. 2011] present *CERTICLOUD*, a solution that builds on a trusted platform module to protect and verify the integrity of IaaS providers. CERTICLOUD is based on two protocols: *i) TPM-based Certification of a Remote Resource* (TCRR) verifies the integrity of physical resources, *ii) VerifyMyVM* verifies the integrity of the environment of the user when deployed in the cloud. Muñoz and Maña [Muñoz and Maña 2013] introduce a solution to security certification in the cloud that combines software and hardware-based certification. The proposed approach is based on trusted computing technology, and aims to bridge the gap between cloud certification and trusted computing. Krotsiani et al. [Krotsiani et al. 2013] propose an approach to the incremental certification of cloud services. The proposed approach targets all layers of the cloud stack and is based on continuous monitoring. Cimato et al. [Cimato et al. 2013] introduce a conceptual framework supporting the specification of basic, hybrid, and incremental models for the certification of cloud-based services. In particular, they define a meta-model supporting the management of the whole certification process: from security property definition, to evidence generation and certificate lifecycle management.

5.4. Cloud Audit/Compliance

Another important aspect of cloud assurance is the capability of observing the cloud behavior and evaluating its compliance with customer policies and law regulations. In other words this goal can be expressed with the slogan “making the cloud auditable”. Audit solutions can increase the transparency of the cloud, thus increasing the level of trustworthiness between the cloud itself and its tenants. Specifically, Haeberlen [Haeberlen 2010] and Paerson [Pearson 2011] respectively claim the need of an accountable cloud, which helps to increase users’ trust, and supports both providers and customers in the identification of responsibilities in case of disputes and problems. Later, Rasheed [Rasheed 2013] provided an overview of the state of the art in cloud auditing, focusing on *i)* user requirements, *ii)* techniques for security auditing, and *iii)* capabilities of cloud service providers to address audit requirements.

Wang et al. [Wang et al. 2010; Wang et al. 2013b] use a homomorphic authenticator with random masking to provide an auditing system for the cloud with privacy in mind.

Mei et al. [Mei et al. 2013] present *TTP-ACE*, a trusted third party-based auditing system for the cloud. TTP-ACE is aimed at increasing accountability of cloud service providers and protecting the cloud users. A number of public auditing solutions that do not rely on a TTP have become available. In a seminal paper, Wang et al. [Wang et al. 2011] propose a system supporting integrity verification and addressing the dynamic evolution of data files. Then, Wang et al. [Wang et al. 2012] introduce an integrity auditing mechanism that relies on distributed erasure-coded data. A priori encoding of data permits users to audit a cloud storage at low computation and communication costs. After that, Wang et al. [Wang et al. 2013] designed a complete public auditing mechanism for the cloud. Their approach guarantees shared data integrity as well as efficient revocation of users using proxy re-signatures. Public verifiers are then capable of auditing data integrity with no need to retrieve the entire data from the cloud. Recently, Wang et al. [Wang et al. 2014] proposed an approach to privacy-preserving public auditing, which supports integrity verification of shared data in the cloud. The proposed solution is based on a ring signature that protects the identity of the signers from public auditors, and allows integrity verification without requiring the disclosure of the entire file. Birnbaum et al. [Birnbaum et al. 2013] introduce a new behavioral modeling scheme to audit VM behaviors and detect suspicious processes. The proposed cloud security auditing solution has been evaluated on a private cloud computing platform. Rajkumar et al. [Rajkumar et al. 2013] describe an efficient auditing approach based on raptor codes that provides data integrity in the cloud. The same approach also supports functionalities for recovering data in case of failures. Shetty [Shetty 2013] considers the analysis of network traffic as a fundamental aspect of cloud auditing to the aim of verifying security of data exchanged between a cloud provider and users. The proposed approach is based on IP geolocation of network devices, monitoring data security in the network, and analysis of large cloud auditing logs. Yang and Jia [Yang and Jia 2013] define an auditing framework for cloud storage, which ensures that data have been saved following agreements with data owners. They also provide a secure and privacy-preserving auditing protocol, with no trusted parties, which supports dynamic operations and batch auditing. Ni et al. [Ni et al. 2014] show that the auditing protocol in [Yang and Jia 2013] is insecure against active adversaries in the cloud, and that adversaries can modify cloud data without being detected. They also propose a solution to solve the problem, preserving all properties of the original protocol. Doelitzscher et al. [Doelitzscher et al. 2012; Doelitzscher et al. 2013] propose *Security Audit as a Service* (SAaaS), a cloud audit and incident detection system. Their goal is to present a solution that *i)* addresses the limitations of traditional audit and intrusion detection systems when moved to the cloud and *ii)* reacts to changes in the cloud infrastructure. SAaaS is aimed at increasing transparency of cloud by giving customers access to data about security incidents. In a later development [Doelitzscher et al. 2013], the authors presented a cloud audit policy language for the SAaaS architecture, which aims to enrich SAaaS towards the definition of a complete audit system. The presented approach mostly targets IaaS level, is focused on security monitoring, and is aimed at presenting auditing data through a standard interface. Zhu et al. [Zhu et al. 2013] propose a dynamic audit service relying on an index-hash table that supports provable updates to outsourced data. Dynamic auditing guarantees timely anomaly detection. Zawoad et al. [Zawoad et al. 2013] present *Secure-Logging-as-a-Service* (SecLaaS), a logging system that provides VM logs to forensic investigators preserving privacy and confidentiality of cloud users. Also, SecLaaS preserves log integrity from dishonest investigators or cloud providers. Recently, Cloud Security Alliance (CSA) started an effort called *CloudAudit* [CSA 2014], which focuses on the provisioning of a common interface and namespace supporting enterprises in the management of their internal audit processes.

5.5. Service Level Agreement (SLA)

Another class of assurance techniques is based on Service Level Agreements (SLAs). SLA-based techniques aim to establish contracts between clients and service providers regulating their interactions, and modeling their expectations in terms of both functional and non-functional agreements. Wieder et al. [Wieder et al. 2011] provide an overview of the usage of SLAs in the cloud and service-oriented architectures. Existing techniques mainly focus on SLA management and negotiation (e.g., [Wieder et al. 2011; Bernsmed et al. 2011; Sakr and Liu 2012; CIO 2012; Jhawar and Piuri 2013]) and approaches to service selection based on QoS and non-functional properties (e.g., [Zhao et al. 2012; Garg et al. 2013; Mouratidis et al. 2013]). In a whitepaper [CIO 2012], the CIO Council and the Chief Acquisition Officers Council discuss guidelines for setting up cloud computing contracts that can be effectively consumed in a federal government scenario. The paper also describes requirements on cloud computing contracts, based on the input provided by different working groups, allowing US agencies to effectively and safely select and consume cloud services.

Several frameworks have been proposed for cloud SLAs. Bernsmed et al. [Bernsmed et al. 2011] present a framework for the management of security SLAs in the cloud, focusing on hybrid clouds and federated cloud services. The framework aims to support service composition based on security requirements and increase cloud trustworthiness. The paper also specifies the SLA lifecycle and the negotiation flow. Sakr and Liu [Sakr and Liu 2012] present a middleware-based framework to SLA-based provisioning in the context of cloud-hosted databases. The proposed framework supports dynamic provisioning of the data layer, and relies on application-specific policies matching customer's performance requirements defined with SLAs. Ye et al. [Ye et al. 2012] propose a framework based on a third party auditor for the verification of SLAs between users and cloud service providers. A testing algorithm within the framework has been designed to detect SLA violations on VM physical memory size. As QoS is an important part of SLA, Garg et al. [Garg et al. 2013] propose the *Service Measurement Index Cloud* (SMICloud) framework that supports cloud users in the identification of the most suitable cloud provider and in the management of SLAs. SMICloud implements different functionalities including QoS-based selection and ranking of cloud services according to their quality, previous user experiences, and performance. SMICloud can foster competition among service providers increasing the quality of cloud services. Zhao et al. [Zhao et al. 2012] propose an architecture for QoS-based service selection in SOAs and cloud. The proposed solution is flexible, scalable, and supports multiple objectives and user personalization. Marinescu et al. [Marinescu et al. 2013] provide a novel cloud delivery model based on combinatorial auctions supporting a better management of QoS and security, while Casalicchio and Silvestri [Casalicchio and Silvestri 2013] analyze the problem of self-adaptable solutions to cloud resource management that react to workload changes and new utility principles. The authors put forward the example of a service supplier moving services to the cloud in order to benefit from a scalable provisioning that addresses QoS constraints. Instead of focusing on QoS in general, Jin et al. [Jin et al. 2013] describe a method to evaluate availability in virtualized cloud systems and guarantee agreed SLAs. Jhawar and Piuri [Jhawar and Piuri 2013] consider the problem of guaranteeing user availability and performance requirements in the cloud. They propose an adaptive resource management solution based on Markov chains and queues, which restores user requirements in case of failure and recovery events. Other solutions include the work of Mouratidis et al. [Mouratidis et al. 2013], the work of Sulistio and Reich [Sulistio and Reich 2013], and the work of Anisetti et al. [Anisetti et al. 2014]. Mouratidis et al. [Mouratidis et al. 2013] present an advanced solution to the selection of cloud providers on the basis of

security and privacy requirements. Their paper proposes a modeling language and a structured process for security- and privacy-aware selection of cloud providers. Sulistio and Reich [Sulistio and Reich 2013] present a solution supporting small-medium enterprises in their migration to the cloud. The service migration approach is based on pre-defined SLA templates and risk analysis. It also provides a self-protecting cloud service that monitors privacy issues and protection mechanisms. Recently, Anisetti et al. [Anisetti et al. 2014] defined a solution for multi-cloud service provisioning. Their approach models service provisioning as *procurement e-auctions*, where a preference relation maps on a partial order of bids. The e-auction mechanism at the basis of the service selection process supports trustworthy bids and improves the truthfulness of the e-auction outcome.

5.6. Discussion

This section surveyed a number of research works aimed to increase the assurance provided to actors at all layers of the cloud stack, evaluating whether a service/cloud stack complies with actors' functional and non-functional requirements. In particular, we presented a set of papers whose main goal is to increase cloud assurance on the security mechanisms and controls discussed in Section 4.

Table III presents our main findings. First of all, we note that since assurance techniques are relatively more recent than security techniques, it is difficult to categorize them according to the security properties they target. In fact, current approaches mainly focus on providing general-purpose assurance techniques rather than focusing on specific security aspects. As a consequence, Table III only lists relevant papers according to the classification of assurance techniques in Section 2.2. Furthermore, we note that testing, monitoring, and SLA solutions were obtained by adapting existing solutions to the cloud environment. Indeed, testing approaches have focused on testing cloud-based applications and on a testing-as-a-service approach, where a testing tool is deployed in the cloud and used to verify any software/service. Monitoring approaches, instead, focused on requirements for the deployment of a monitoring infrastructure in the cloud. Approaches based on SLA have focused on SLA-aware cloud provisioning, with the aim of supporting QoS-based service selection. Finally, some approaches have started considering the problem of verifying properties of cloud services/stacks using certification-based approaches (a priori) or auditing solutions (a posteriori).

6. DISCUSSION

Reviewed contributions varied in type, covered various aspects of cloud security and assurance, and have been selected according to the methodology described in Section 2. Now we present the results of our survey (Section 6.1) and some recommendations for next generation security solutions in the cloud (Section 6.2).

6.1. Cloud security and assurance: Overview of the results

We surveyed a total of 306 works (including the ones in the appendices) among which 31 present surveys and whitepapers, 21 describe standards and research projects, 161 illustrate research papers focusing on specific aspects of security and assurance in the cloud, and the remaining are papers considering either general aspects of cloud environments and distributed systems, or security vulnerabilities, threats, and attacks. We then focused our study on the 161 research papers analyzing the status of the research in the field of cloud security and assurance. A more detailed summary of the 161 research papers according to the methodology in Section 2 is provided in Appendix B.

Figure 2 presents an overview of the status of cloud security and assurance on the basis of the surveyed papers. Figure 2(a) presents the distribution of papers in the period 2009 and 2014, distinguishing between security and assurance approaches. To

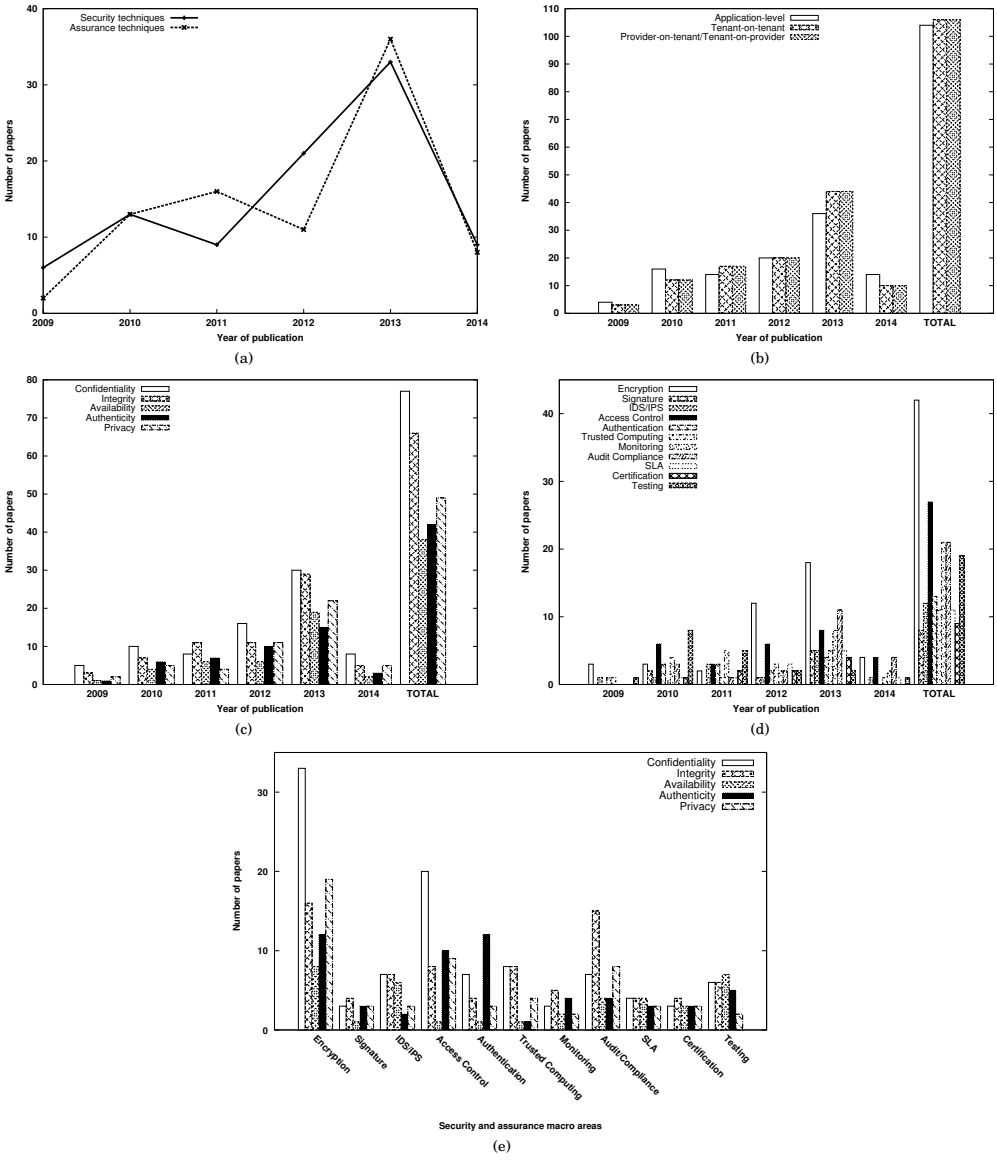

Fig. 2. Security and assurance techniques distribution in period 2009-2014

correctly evaluate the distribution of papers in Figure 2(a), we recall that in this survey we favored recent papers (after 2012). Taking into consideration the last 3-year period, we can observe that the growth in the number of assurance-oriented papers between 2012 and 2013 is much higher (from 13% to 42% of the total number of solutions in the period 2009-2014) than the growth in the number of security-oriented papers (from 23% to 36%). This is more evident if we consider absolute numbers: we analyzed 11 assurance-oriented papers in 2012 and 36 papers in 2013, while we studied 21 security oriented papers in 2012 and 33 in 2013. Finally, it is important to note that the number of papers analyzed in 2013 and 2014 distributes almost equally between security and assurance techniques, showing that assurance is increasingly considered

by the research community as an important aspect, and is becoming as important as security in the cloud.

Figure 2(b) shows the trend of security and assurance techniques with respect to the attack surface. First of all, we note that more work has been done on solutions considering application-level (34.9%) and tenant-on-tenant (35.6%) attack surfaces, while less work is available on provider-on-tenant and tenant-on-provider attack surface (29.5%). This is due to the fact that application-level solutions often are straightforward evolutions of approaches defined for service-oriented architectures, while tenant-on-tenant attacks have been modeled since long. These data are even more clear if we consider that *i)* more than 50% of the work focusing on provider-on-tenant and tenant-on-provider also considers the other two attack surfaces and *ii)* more than 78% focuses on at least one of the other two surfaces. Also, we note that the number of defined solutions is increasing for all attack surface categories with similar trends.

Figure 2(c) shows that, as expected, existing techniques put more effort on preserving/protecting confidentiality (28.3%) and integrity (24.3%) properties, while less effort has been done on availability (14%), authenticity (15.4%), and privacy (18%). These results confirm the importance of guaranteeing confidentiality and integrity of user data and applications when moved to the cloud, but also the need of additional research on identity management solutions operating across clouds. We also note that the relatively low number of solutions targeting availability is due to the fact that availability is often seen as a property at the border between the security, reliability, and performance research areas. In addition, Figure 2(c) shows that the number of defined solutions is increasing for all security properties with similar trends.

Figure 2(d) show that encryption (37.2%) and access control (23.9%) are the preferred classes of techniques for implementing cloud security approaches. The above classes are completed (and more often integrated) with approaches relying on digital signature (7.1%) and authentication (11.5%), respectively. Less work instead has been done on IDS/IPS (10.6%) and trusted computing (9.7%), because both techniques have been proposed only recently for virtual environments. Furthermore, it is rather complex to employ trusted computing since it requires the support of special hardware devices and its deployment cost is high. The same remark can be done on IDS/IPS that when moved to the cloud introduce higher management and configuration overheads. Considering cloud security assurance, the distribution of techniques in the classes defined in Section 2.2 is broken in two sets. The first one includes audit, monitoring, and testing approaches having the greatest percentage of implemented techniques (25.9%, 25.9%, 23.5%, resp.). The second one includes SLA and certification having the lowest rate (13.6% and 11.1%, resp.). The success of auditing, monitoring, and testing classes is due to the fact that their techniques are often used to verify functionalities of distributed infrastructures and can then be easily applied to a cloud environment. Also, very often the cloud infrastructure has been used to deliver monitoring and testing functionalities as a service. By contrast, SLA and certification approaches have been applied to service environments only recently and therefore are still only occasionally used in cloud infrastructures.

Finally, Figure 2(e) gives an overview of how different techniques distribute among targeted properties. If we consider security techniques, 34.8% target confidentiality property (highest), while only 8% target availability property (lowest). The remaining techniques almost equally target integrity, authenticity, and privacy properties (between 17.9% and 21%). If we consider assurance techniques, their distribution is more homogeneous among classes of properties, probably because they have been applied to cloud environments only recently: 29.8% for integrity (highest) and 15.8% for privacy (lowest).

6.2. Recommendations for next-generation cloud security and assurance

Widespread adoption of cloud computing requires security and assurance solutions increasing the trust of cloud users in the cloud itself and in cloud providers. The problem of enforcing and verifying security is exacerbated by the fact that the cloud provides many functionalities increasing flexibility, performance, and reliability (e.g., migration, federation, scalability, elasticity), which affect the functioning of security and assurance solutions for distributed networks.

Many researchers have proposed fine-grained security solutions that target different angles of the cloud security problem. Although such solutions might help expert users to secure their applications and data in the cloud, they make the cloud security scenario cumbersome for the majority of customers.

According to [Ardagna et al. 2014], we claim that *introspection*, which is the capability of a cloud provider of examining and observing its internal processes, is not the only concept that matters when considering cloud security. In fact, the concept of *outrospection*, that is, empowering customers and service providers with the ability to examine and observe cloud's internal processes impacting on (the security of) their activities/applications/data, is also of paramount importance. A proper solution to security in the cloud should embrace both introspection by cloud providers and outrospection by cloud customers (tenants in general), balancing security and assurance control between providers and customers, and fostering full adoption of the cloud paradigm also in critical environments. We claim that an increased cloud transparency can help the security management problem, supporting both introspection and outrospection. Transparency can be achieved via standardized interfaces, independent from the cloud stack, which give a common access point to events and activities happening in the cloud back-end. For instance, support for a given security property can be proven, monitored, and tested by collecting data on the functioning of a given security mechanism (e.g., an access control mechanism for authorization). By collecting uniform and homogeneous data on cloud activities, we can also enrich solutions evaluating cloud compliance and audit, as well as approaches supporting dynamic adaptation of the cloud infrastructure to changes that would affect both the cloud provider (and its management activities) and the customer (and the corresponding services). Also, standardized access to these data can give to the customers some evidence on the current status of their services and overall security, and support the management of their security (and more in general non-functional) property life-cycle.

Cloud back-end data represent a hidden treasure over which one can build new services, and improve cloud functionality, security, and assurance.

REFERENCES

G. Aceto, A. Botta, W. De Donato, and A. Pescapè. 2013. Cloud Monitoring: A Survey. *Computer Networks* 57, 9 (June 2013), 2093–2115.

Advanced Security Service cERTificate for SOA 2010. *Advanced Security Service cERTificate for SOA*. http://assert4soa.eu/.

E. Aguiar, Y. Zhang, and M. Blanton. 2013. An Overview of Issues and Recent Developments in Cloud Computing and Storage Security. In *High Performance Semantic Cloud Auditing*, B.-Y. Choi, K. Han, and S. Song (Eds.). Springer.

M. Ahmed, Q.H. Vu, R. Asal, H. Al Muhairi, and C.Y. Yeun. July 2012. SECRESO: a Secure Storage Model for Cloud Data based on Reed-Solomon Code. In *Proc. of AIM 2012*. Jeju, South Korea.

M. Al Morsy, J. Grundy, and I. Müller. November-December 2010. An Analysis of The Cloud Computing Security Problem. In *Proc. of APSEC-CLOUD 2010*. Sydney, Australia.

K. Alhamazani, R. Ranjan, K. Mitra, F. Rabhi, S.U. Khan, A. Guabtni, and V. Bhatnagar. 2013. An Overview of the Commercial Cloud Monitoring Tools: Research Dimensions, Design Issues, and State-of-the-Art. *CoRR* abs/1312.6170 (2013).

S.A. Almulla and C.Y. Yeun. March-April 2010. Cloud computing security management. In *Proc. of ICESMA 2010*. Sharjah, UAE.

S. Andreozzi, N. De Bortoli, S. Fantinel, A. Ghiselli, G. Rubini, G. Tortone, and M.C. Vistoli. 2005. GridICE: a monitoring service for Grid systems. *Future Generation Computer Systems* 21, 4 (April 2005), 559–571.

Aniketos, ASSERT4SOA, CUMULUS, SecCord. 2013. *Specifications identification & gap analysis Use cases 43, 78, 80*. http://csc.etsi.org/Application/documentapp/downloadimmediate/?docId=123.

M. Anisetti, C.A. Ardagna, and E. Damiani. June 2012. A Low-Cost Security Certification Scheme for Evolving Services. In *Proc. of IEEE ICWS 2012*. Honolulu, HI, USA.

M. Anisetti, C.A. Ardagna, and E. Damiani. June-July 2013a. Security Certification of Composite Services: A Test-Based Approach. In *Proc. of IEEE ICWS 2013*. San Francisco, CA, USA.

M. Anisetti, C.A. Ardagna, E. Damiani, P.A. Bonatti, M. Faella, C. Galdi, and L. Sauro. 2014. e-Auctions for Multi-Cloud Service Provisioning. In *Proc. of IEEE SCC 2014*. Anchorage, AL, USA.

M. Anisetti, C.A. Ardagna, E. Damiani, and F. Saonara. 2013b. A Test-based Security Certification Scheme for Web Services. *ACM TWEB* 7, 2 (May 2013), 1–41.

C.A. Ardagna, R. Asal, E. Damiani, and Q.H. Vu. March-April 2014. On the Management of Cloud Non-Functional Properties: The Cloud Transparency Toolkit. In *Proc. of IFIP NTMS 2014*. Dubai, UAE.

C.A. Ardagna, E. Damiani, F. Frati, D. Rebeccani, and M. Ughetti. June 2012. Scalability Patterns for Platform-as-a-Service. In *Proc. of IEEE CLOUD 2012*. Honolulu, HI, USA.

M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. 2009. Above the clouds: A Berkeley view of cloud computing. In *Tech. Rep. UCB/EECS-2009-28*. EECS Department, U.C. Berkeley.

M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. 2010. A View of Cloud Computing. *CACM* 53, 4 (April 2010), 50–58.

W.W. Armour et al. 2013. *NIST Cloud Computing Security Reference Architecture*. NIST Special Publication 500-299, http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/CloudSecurity/NIST_Security_Reference_Architecture_2013.05.15_v1.0.pdf.

V. Attasena, N. Harbi, and J. Darmont. September 2013. Sharing-based Privacy and Availability of Cloud Data Warehouses. In *Proc. of EDA 2013*. Leuven, Belgium.

A. Aviram, S. Hu, B. Ford, and R. Gummadi. October 2010. Determinating Timing Channels in Compute Clouds. In *Proc. of ACM CCSW 2010*. Chicago, IL, USA.

J. Bacon, D. Eyers, T. Pasquier, J. Singh, I. Papagiannis, and P. Pietzuch. 2014. Information Flow Control for Secure Cloud Computing. *IEEE TNSM* (2014).

X. Bai, M. Li, B. Chen, W.-T. Tsai, and J. Gao. December 2011. Cloud testing tools. In *Proc. of IEEE SOSE 2011*. Irvine, CA, USA.

X. Bai, M. Li, X. Huang, W.-T. Tsai, and J. Gao. May 2013. Vee@Cloud: The virtual test lab on the cloud. In *Proc. of AST 2013*. San Francisco, CA, USA.

G. Ballabio. 2013. Security and availability techniques for cloud-based applications. *Computer Fraud & Security* 2013, 10 (October 2013), 5–7.

L. Baresi and S. Guinea. December 2005. Dynamo: Dynamic Monitoring of WS-BPEL Processes. In *Proc. of ICSOC 2005*. Amsterdam, The Netherlands.

A. Barsoum and A. Hasan. 2013. Enabling Dynamic Data and Indirect Mutual Trust for Cloud Computing Storage Systems. *IEEE TPDS* 24, 12 (December 2013), 2375–2385.

F. Benali, N. Bennani, G. Gianini, and S. Cimato. October 2010. A Distributed and Privacy-Preserving Method for Network Intrusion Detection. In *Proc. of OTM 2010*. Hersonissos, Crete, Greece.

N. Bennani, E. Damiani, and S. Cimato. July 2010. Toward cloud-based key management for outsourced databases. In *Proc. of SAPSE 2010*. Seoul, South Korea.

S. Berger, R. Cáceres, K.A. Goldman, R. Perez, R. Sailer, and L. van Doorn. July-August 2006. vTPM: Virtualizing the Trusted Platform Module. In *Proc. of USENIX-SS 2006*. Vancouver, B.C., Canada.

K. Bernsmed, M.G. Jaatun, P.H. Meland, and A. Undheim. August 2011. Security SLAs for Federated Cloud Services. In *Proc. of ARES 2011*. Prague, Cezch Republic.

K. Bernsmed, M.G. Jaatun, P.H. Meland, and A. Undheim. December 2012. Thunder in the Clouds: Security challenges and solutions for federated Clouds. In *Proc. of IEEE CloudCom 2012*. Taipei, Taiwan.

B. Bertholon, S. Varrette, and P. Bouvry. July 2011. Certicloud: A Novel TPM-based Approach to Ensure Cloud IaaS Security. In *Proc. of IEEE CLOUD 2011*. Washington, DC, USA.

R. Bhadauria and S. Sanyal. 2012. *Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques*. http://arxiv.org/ftp/arxiv/papers/1204/1204.0764.pdf.

D. Bianculli and C. Ghezzi. September 2007. Monitoring Conversational Web Services. In *Proc. of IW-SOSWE 2007*. Dubrovnik, Croatia.

A. Birgisson, J.G. Politz, U. Erlingsson, A. Taly, M. Vrable, and M. Lentczner. February 2014. Macaroons: Cookies with Contextual Caveats for Decentralized Authorization in the Cloud. In *Proc. of NDSS 2014*. San Diego, CA, USA.

Z. Birnbaum, B. Liu, A. Dolgikh, Y. Chen, and V. Skormin. June-July 2013. Cloud Security Auditing Based on Behavioral Modeling. In *Proc. of IEEE SERVICES 2013*. Santa Clara, CA, USA.

A. Bisong and S.M. Rahman. 2011. An Overview of the Security Concerns in Enterprise Cloud Computing. *CoRR* abs/1101.5613 (2011). http://arxiv.org/abs/1101.5613.

S. Bleikertz, S. Bugiel, H. Ideler, S. Nürnberger, and A.-R. Sadeghi. June 2013. Client-Controlled Cryptography-as-a-Service in the Cloud. In *Proc. of ACNS 2013*. Banff, AB, Cananda.

S. Bleikertz, A. Kurmus, Z.A. Nagy, and M. Schunter. May 2012. Secure cloud maintenance: protecting workloads against insider attacks. In *Proc. of ACM ASIACCS 2012*. Seoul, Korea.

P.A. Boampong and L.A. Wahsheh. March 2012. Different Facets of Security in the Cloud. In *Proc. of CNS 2012*. Orlando, FL, USA.

J.-M. Bohli, N. Gruschka, M. Jensen, L.L. Iacono, and N. Marnau. 2013. Security and Privacy-Enhancing Multicloud Architectures. *Dependable and Secure Computing, IEEE Transactions on* 10, 4 (July-August 2013), 212–224.

G. Booth, A. Soknacki, and A. Somayaji. June 2013. Cloud Security: Attacks and Current Defenses. In *Proc. of ASIA 2013*. Albany, NY, USA.

P. Bosc, E. Damiani, and M. Fugini. 2001. Fuzzy service selection in a distributed object-oriented environment. *IEEE TFS* 9, 5 (2001), 682–698.

S. Bouchenak, G. Chockler, H. Chockler, G. Gheorghe, N. Santos, and A. Shraer. 2013. Verifying Cloud Services: Present and Future. *ACM SIGOPS Operating Systems Review* 47, 2 (July 2013), 6–19.

K.D. Bowers, A. Juels, and A. Oprea. November 2009. HAIL: A High-availability and Integrity Layer for Cloud Storage. In *Proc. of ACM CCS 2009*. Chicago, IL, USA.

N. Brender and I. Markov. 2013. Risk perception and risk management in cloud computing: Results from a case study of Swiss companies. *IJIM* 33, 5 (June 2013), 726–733.

J. Buckley, T. Mens, M. Zenger, A. Rashid, and G. Kniesel. 2005. Towards a Taxonomy of Software Change: Research Articles. *Journal of Software Maintenance and Evolution: Research and Practice - Unanticipated Software Evolution* 17, 5 (September 2005), 309–332.

S. Bugiel, S. Nürnberger, T. Pöppelmann, A.-R. Sadeghi, and T. Schneider. October 2011. AmazonIA: When Elasticity Snaps Back. In *Proc. of ACM CCS 2011*. Chicago, IL, USA.

R.A. Burger, C. Cachin, and E. Husmann. 2013. *Cloud, Trust, Privacy*.

T. Caddy. 2011. Side-Channel Attacks. In *Encyclopedia of Cryptography and Security*, H.C.A. van Tilborg and S. Jajodia (Eds.). Springer.

G. Candea, S. Bucur, and C. Zamfir. June 2010. Automated Software Testing As a Service. In *Proc. of ACM SoCC 2010*. Indianapolis, IN, USA.

B. Carminati. 2009. Merkle Trees. In *Encyclopedia of Database Systems*, L. Liu, M.T. Özsu, and M. Tamer (Eds.). Springer.

E. Casalicchio and L. Silvestri. 2013. Mechanisms for SLA Provisioning in Cloud-based Service Providers. *Computer Networks* 57, 3 (February 2013), 795–810.

D. Catteddu and G. Hogben. November 2009a. *Cloud Computing: Benefits, Risks and Recommendations for Information Security*. European Network and Information Security Agency (ENISA). http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport.

D. Catteddu and G. Hogben. November 2009b. *Information Assurance Framework*. European Network and Information Security Agency (ENISA). .

CEN. 2014. *CEN Workshop on Requirements and recommendations for assurance in the Cloud (WS RACS)*. http://www.cen.eu/work/areas/ICT/eBusiness/Pages/WS-RACS.aspx.

Certification infrastrUcture for MUlti-layer cloUd Services 2013. *Certification infrastrUcture for MUlti-layer cloUd Services*. http://www.cumulus-project.eu/.

Certification, InteRnationalisation and standaRdization in cloUd Security 2012. *Certification, InteRnationalisation and standaRdization in cloUd Security*. http://www.cirrus-project.eu/.

W.K. Chan, L. Mei, and Z. Zhang. December 2009. Modeling and testing of cloud applications. In *Proc. of IEEE APSCC 2009*. Singapore.

N.S. Chauhan, A. Saxena, and J.V.R. Murthy. October 2013. An Approach to Measure Security of Cloud Hosted Application. In *Proc. of IEEE CCEM 2013*. Bangalore, India.

X. Chen, J. Andersen, Z.M. Mao, M. Bailey, and J. Nazario. June 2008. Towards an understanding of anti-virtualization and anti-debugging behavior in modern malware. In *Proc. of IEEE/IFIP DSN 2008*. Anchorage, AL, USA.

Y. Chen, V. Paxson, and R.H. Katz. January 2010. *What's New About Cloud Computing Security?* Technical Report No. UCB/EECS-2010-5, http://www.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.html.

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

S.S.M. Chow, C.-K. Chu, X. Huang, J. Zhou, and R.H. Deng. 2012. Dynamic Secure Cloud Storage with Provenance. In *Cryptography and Security*, D. Naccache (Ed.). Springer-Verlag, Berlin, Heidelberg, 442–464.

M. Christodorescu, R. Sailer, D.L. Schales, D. Sgandurra, and D. Zamboni. November 2009. Cloud Security is Not (Just) Virtualization Security. In *Proc. of ACM CCSW 2009*. Chicago, Illinois, USA.

C.-K. Chu, S. S. M. Chow, W.-G. Tzeng, J. Zhou, and R. H. Deng. 2014. Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage. *IEEE TPDS* 25, 2 (February 2014), 468–477.

S. Cimato, E. Damiani, F. Zavatarelli, and R. Menicocci. June-July 2013. Towards the Certification of Cloud Services. In *Proc. of IEEE SERVICES 2013*. Santa Clara, CA, USA.

CIO. 2012. *Creating Effective Cloud Computing Contracts for the Federal Government – Best Practices for Acquiring IT as a Service*. Council and Chief Acquisition Officer Council. http://www.gsa.gov/portal/mediaId/164011/fileName/cloudbestpractices.action.

L. Ciortea, C. Zamfir, S. Bucur, V. Chipounov, and G. Candea. 2010. Cloud9: A Software Testing Service. *ACM SIGOPS Operating Systems Review* 43, 4 (January 2010), 5–10.

S. Clayman, A. Galis, C. Chapman, G. Toffetti, L. Rodero-Merino, L. Miguel Vaquero, K. Nagin, and B. Rochwerger. 2010. Monitoring Service Clouds in the Future Internet. In *Towards the Future Internet*, G. Tselentis, A. Galis, A. Gavras, S. Krco, V. Lotz, E. Simperl, B. Stiller, and T. Zahariadis (Eds.). IOS Press, 115–126.

Cloud Accountability Project 2012. *Cloud Accountability Project*. http://www.a4cloud.eu/.

Cloud Security Alliance. 2010. *Guidance for identity & access management V2.1*. http://www.cloudsecurityalliance.org/guidance/csaguide-dom12-v2.10.pdf.

Cloud Security Alliance. 2011. *Security Guidance for Critical Areas of Focus in Cloud Computing V3.0*. https://downloads.cloudsecurityalliance.org/initiatives/guidance/csaguide.v3.0.pdf.

Cloud Security Alliance. 2013. *The Notorious Nine Cloud Computing Top Threats in 2013*. https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf.

Cloud Security on Demand 2012. *Cloud Security on Demand*. http://www.nsf.gov/awardsearch/showAward?AWD_ID=1218817&HistoricalAwards=false.

Cloud Standards Customer Council. August 2012. *Security for Cloud Computing 10 Steps to Ensure Success*. http://www.cloud-council.org/Security_for_Cloud_Computing-Final_080912.pdf.

CloudSec. October 2013. *A Briefing on Cloud Security Challenges and Opportunities*. http://www.telenor.com/wp-content/uploads/2013/11/TelenorWhitepaperCloud-V_30_v.pdf.

Continuous Quality Assurance and Optimisation for Cloud brokers 2012. *Continuous Quality Assurance and Optimisation for Cloud brokers*. http://www.broker-cloud.eu/.

CSA. 2014. *CloudAudit: Automated Audit, Assertion, Assessment, and Assurance*. https://cloudsecurityalliance.org/research/cloudaudit/.

K. Dahbur, B. Mohammad, and A.B. Tarakji. April 2011. A Survey of Risks, Threats and Vulnerabilities in Cloud Computing. In *Proc. of ISWSA 2011*. Amman, Jordan.

E. Damiani, C.A. Ardagna, and N. El Ioini. 2009a. *Open source systems security certification*. Springer, New York, NY, USA.

E. Damiani, N. El Ioini, A. Sillitti, and G. Succi. July 2009b. WS-Certificate. In *Proc. of IEEE SERVICES I 2009*. Los Angeles, CA, USA.

W. Dawoud, I. Takouna, and C. Meinel. March 2010. Infrastructure as a service security: Challenges and solutions. In *Proc. of INFOS 2010*. Cairo, Egypt.

S. De Capitani di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati. 2013. Integrity for Join Queries in the Cloud. *IEEE TCC* 1, 2 (July-December 2013), 187–200.

S. De Capitani di Vimercati, S. Foresti, and P. Samarati. 2014. Selective and Fine-Grained Access to Data in the Cloud. In *Secure Cloud Computing*, S. Jajodia, K. Kant, P. Samarati, V. Swarup, and C. Wang (Eds.). Springer.

M. Dekker and G. Hogben. December 2011. *Survey and analysis of security parameters in cloud SLAs across the European public sector*. European Network and Information Security Agency (ENISA). http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/survey-and-analysis-of-security-parameters-in-cloud-slas-across-the-european-public-sector/at_download/fullReport.

Y. Desmedt. 2011. Covert Channels. In *Encyclopedia of Cryptography and Security*, H.C.A. van Tilborg and S. Jajodia (Eds.). Springer.

M.H. Diallo, B. Hore, E.-C. Chang, S. Mehrotra, and N. Venkatasubramanian. June 2012. CloudProtect: Managing Data Privacy in Cloud Applications. In *Proc. of IEEE CLOUD 2012*. Honolulu, HI, USA.

F. Doelitzscher, C. Reich, M. Knahl, and N. Clarke. 2013. Understanding Cloud Audits. In *Privacy and Security for Cloud Computing*, S. Pearson and G. Yee (Eds.). Springer London, 125–163.

F. Doelitzscher, C. Reich, M. Knahl, A. Passfall, and N. Clarke. 2012. An agent based business aware incident detection system for cloud environments. *JoCCASA* 1, 1 (2012), 1–19.

F. Doelitzscher, T. Ruebsamen, T. Karbe, M. Knahl, C. Reich, and N. Clarke. 2013. Sun Behind Clouds - On Automatic Cloud Security Audits and a Cloud Audit Policy Language. *International Journal on Advances in Networks and Services* 6, 1–2 (2013), 1–16.

A. Donevski, S. Ristov, and M. Gusev. May 2013. Security assessment of virtual machines in open source clouds. In *Proc. of MIPRO 2013*. Opatija, Croatia.

D. Dranidis, E. Ramollari, and D. Kourtesis. November 2009. Run-time Verification of Behavioural Conformance for Conversational Web Services. In *Proc. of IEEE ECOWS 2009*. Eindhoven, The Netherlands.

G. Dsouza, G. Rodriguez, Y. Al-Nashif, and S. Hariri. 2013. Building resilient cloud services using DDDAS and moving target defence. *JCC* 2, 2/3 (2013), 171–190.

Empowering the service industry with SLA-aware infrastructures 2008. *Empowering the service industry with SLA-aware infrastructures*. http://sla-at-soi.eu/.

Ensuring Trustworthiness and Security in Service Composition 2010. *Ensuring Trustworthiness and Security in Service Composition*. http://www.aniketos.eu/.

ETSI. November 2013. *Cloud Standards Coordination – Final Report*. http://csc.etsi.org/Application/documentapp/downloadimmediate/?docId=204.

D.A.B. Fernandes, L.F.B. Soares, J.V. Gomes, M.M. Freire, and P.R.M. Inacio. 2013. Security issues in cloud environments: a survey. *International Journal of Information Security* (September 2013), 1–58.

M. Ficco, L. Tasquier, and R. Aversa. October 2013. Intrusion Detection in Cloud Computing. In *Proc. of 3PGCIC 2013*. Compiegne, France.

R. Focardi, R. Gorrieri, and F. Martinelli. 2004. Classification of Security Properties (Part II: Network Security). In *Foundations of Security Analysis and Design II - Tutorial Lectures*, R. Focardi and R. Gorrieri (Eds.). Springer Berlin / Heidelberg.

H. Foster and G. Spanoudakis. March 2011a. Advanced Service Monitoring Configurations with SLA Decomposition and Selection. In *Proc. of ACM SAC 2011*. TaiChung, Taiwan.

H. Foster and G. Spanoudakis. May 2011b. SMaRT: A Workbench for Reporting the Monitorability of Services from SLAs. In *Proc. of PESOS 2011*. Honolulu, HI, USA.

Ganglia. 2014. http://ganglia.sourceforge.net/.

J. Gao, X. Bai, and W.-T. Tsai. 2011. Cloud Testing-Issues, Challenges, Needs and Practice. *SeiJ* 1, 1 (September 2011).

J. Gao, X. Bai, W.-T. Tsai, and T. Uehara. 2013. SaaS Testing on Clouds - Issues, Challenges and Needs. *Proc. of IEEE SOSE 2013* (March 2013).

S.K. Garg, S. Versteeg, and R. Buyya. 2013. A framework for ranking of cloud computing services. *Future Generation Computer Systems* 29, 4 (June 2013), 1012–1023.

German Federal Office for Information Security. August 2012. *Security Recommendations for Cloud Computing Providers*. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Minimum_information/SecurityRecommendationsCloudComputingProviders.pdf?__blob=publicationFile.

E. Ghazizadeh, J.-L.A. Manan, M. Zamani, and A. Pashang. December 2012. A survey on security issues of federated identity in the cloud computing. In *Proc. of IEEE CloudCom 2012*. Taipei, Taiwan.

C. Ghezzi and S. Guinea. 2007. Run-Time Monitoring in Service-Oriented Architectures. In *Test and Analysis of Web Services*, L. Baresi and E. Di Nitto (Eds.). Springer Berlin Heidelberg, 237–264.

M. Godfrey and M. Zulkernine. June 2013. A Server-Side Solution to Cache-Based Side-Channel Attacks in the Cloud. In *Proc. of IEEE CLOUD 2013*. Santa Clara, CA, USA.

M. Green. 2013. The Threat in the Cloud. *IEEE Security & Privacy* 11, 1 (January-February 2013), 86–89.

B. Grobauer, T. Walloschek, and E. Stocker. 2011. Understanding Cloud Computing Vulnerabilities. *IEEE Security & Privacy* 9, 2 (March-April 2011), 50–57.

N. Gruschka and L.L. Iacono. July 2009. Vulnerable Cloud: SOAP Message Security Validation Revisited. In *Proc. of IEEE ICWS 2009*. Los Angeles, CA, USA.

N. Gruschka and M. Jensen. July 2010. Attack Surfaces: A Taxonomy for Attacks on Cloud Services. In *Proc. of IEEE CLOUD 2010*. Miami, FL, USA.

A. Haeberlen. 2010. A Case for the Accountable Cloud. *ACM SIGOPS Operating Systems Review* 44, 2 (April 2010), 52–57.

S. Hallé and R. Villemaire. March 2009. Runtime Monitoring of Web Service Choreographies Using Streaming XML. In *Proc. of ACM SAC 2009*. Honolulu, HI, Hawaii.

W.M. Halton and S. Rahman. 2012. The Top Ten Cloud-security Practices in Next-generation Networking. *IJCNDS* 8, 1/2 (December 2012), 70–84.

T. Hanawa, T. Banzai, H. Koizumi, R. Kanbayashi, T. Imada, and M. Sato. April 2010. Large-Scale Software Testing Environment Using Cloud Computing Technology for Dependable Parallel and Distributed Systems. In *Proc. of ICSTW 2010*. Paris, France.

Z. Hao, S. Zhong, and N. Yu. 2011. A Time-Bound Ticket-Based Mutual Authentication Scheme for Cloud Computing. *IJCCC* 6, 2 (2011), 227–235.

K. Hashizume, D.G. Rosado, E. Fernndez-Medina, and E.B. Fernandez. 2013. An analysis of security issues for cloud computing. *JISA* 4, 1 (2013), 1–13.

G. Hogben and M. Dekker. 2012. *Procure Secure: A guide to monitoring of security service levels in cloud contracts*. European Network and Information Security Agency (ENISA). http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts/at_download/fullReport.

V. Holub, T. Parsons, P. O'Sullivan, and J. Murphy. June 2009. Runtime correlation engine for system monitoring and testing. In *Proc. of ICAC-INDST 2009*. Barcelona, Spain.

I. Iankoulova and M. Daneva. May 2012. Cloud computing security requirements: A systematic review. In *Proc. of RCIS 2012*. Valencia, Spain.

IATAC and DACS. 2007. *Software Security Assurance: State of the Art Report (SOAR)*. http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA472363.

A.S. Ibrahim, J. Hamlyn-Harris, and J. Grundy. November-December 2010. Emerging Security Challenges of Cloud Virtual Infrastructure. In *Proc. of APSEC-CLOUD 2010*. Sydney, Australia.

Infrastructure for Secure Cloud Computing 2013. *Infrastructure for Secure Cloud Computing*. http://www.nsf.gov/awardsearch/showAward?AWD_ID=1253870&HistoricalAwards=false.

C. Irvine and T. Levin. December 1999. Toward a taxonomy and costing method for security services. In *Proc. of ACSAC 1999*. Phoenix, AZ, USA.

S. Jajodia, W. Litwin, and T. Schwarz. 2013. Recoverable Encryption through a Noised Secret over a Large Cloud. In *Transactions on Large-Scale Data- and Knowledge-Centered Systems IX*, A. Hameurlain, J. Küng, and R. Wagner (Eds.). Lecture Notes in Computer Science, Vol. 7980. Springer Berlin Heidelberg, 42–64.

W. Jansen and T. Grance. 2011. *Guidelines on Security and Privacy in Cloud Computing*. NIST SP-800-144, http://www.nist.gov/manuscript-publication-search.cfm?pub_id=909494.

D. Jayasinghe, G. Swint, S. Malkowski, J. Li, Q. Wang, J. Park, and C. Pu. June 2012. Expertus: A Generator Approach to Automate Performance Testing in IaaS Clouds. In *Proc. of IEEE CLOUD 2012*. Honolulu, HI, USA.

C. Jenkins. 2013. The three pillars of a secure hybrid cloud environment. *Computer Fraud & Security* 2013, 6 (June 2013), 13–15.

M. Jensen, J. Schwenk, N. Gruschka, and L.L. Iacono. July 2009. On Technical Security Issues in Cloud Computing. In *Proc. of IEEE CLOUD 2009*. Los Angeles, CA, USA.

R. Jhawar and V. Piuri. August 2013. Adaptive Resource Management for Balancing Availability and Performance in Cloud Computing. In *Proc. of SECRYPT 2013*. Vienna, Austria.

R. Jhawar, V. Piuri, and P. Samarati. December 2012. Supporting Security Requirements for Resource Management in Cloud Computing. In *Proc. of IEEE CSE 2012*. Paphos, Cyprus.

S. Jin, J. Seol, and S. Maeng. May 2013. Towards Assurance of Availability in Virtualized Cloud System. In *Proc. of IEEE/ACM CCGrid 2013*. Delft, The Netherlands.

A. Juels and A. Oprea. 2013. New Approaches to Security and Availability for Cloud Data. *CACM* 56, 2 (February 2013).

T. Jung, X.-Y. Li, and Z. Wan. April 2013. Privacy Preserving Cloud Data Access With Multi-Authorities. In *Proc. of IEEE INFOCOM 2013*. Turin, Italy.

N. Kaaniche, A. Boudguiga, and M. Laurent. June 2013. ID Based Cryptography for Cloud Data Storage. In *Proc. of IEEE CLOUD 2013*. Santa Clara, CA, USA.

L. Kai, T. Weiqin, Z. Liping, and H. Chao. November 2013. SCM: A Design and Implementation of Monitoring System for CloudStack. In *Proc. of CSC 2013*. Beijing, China.

C. Kalloniatis, V. Manousakis, H. Mouratidis, and S. Gritzalis. April 2013. Migrating into the Cloud: Identifying the Major Security and Privacy Concerns. In *Proc. of IFIP I3E 2013*. Athens, Greece.

S. Kang, J. Lee, H. Jang, H. Lee, Y. Lee, S. Park, T. Park, and J. Song. June 2008. SeeMon: Scalable and Energy-efficient Context Monitoring Framework for Sensor-rich Mobile Environments. In *Proc. of MobiSys 2008*. Breckenridge, CO, USA.

L.M. Kaufman. 2010. Can Public-Cloud Security Meet Its Unique Challenges? *IEEE Security & Privacy* 8, 4 (July-August 2010), 55–57.

U. Khalid, A. Ghafoor, M. Irum, and M.A. Shibli. September 2013. Cloud Based Secure and Privacy Enhanced Authentication & Authorization Protocol. In *Proc. of KES 2013*. Kitakyushu, Japan.

K.M. Khan and Q. Malluhi. 2010. Establishing Trust in Cloud Computing. *IT Professional* 12, 5 (September-October 2010), 20–27.

T.M. King and A.S. Ganti. April 2010. Migrating Autonomic Self-Testing to the Cloud. In *Proc of ICSTW 2010*. Paris, France.

R.B. Knode. 2009. *Digital Trust in the Cloud: Liquid Security in Cloudy Places*. CSC. http://assets1.csc.com/au/downloads/0610_20_Digital_trust_in_the_cloud.pdf.

F. Koeppe and J. Schneider. November-December 2010. Do You Get What You Pay For? Using Proof-of-Work Functions to Verify Performance Assertions in the Cloud. In *Proc. of IEEE CloudCom 2010*. Indianapolis, IN, USA.

D. Kourtesis, E. Ramollari, D. Dranidis, and I. Paraskakis. 2010. Increased reliability in SOA environments through registry-based conformance testing of Web services. *Production Planning & Control* 21, 2 (2010), 130–144.

F.J. Krautheim. June 2009. Private Virtual Infrastructure for Cloud Computing. In *Proc. of HotCloud 2009*. San Diego, CA, USA.

M. Krotsiani, G. Spanoudakis, and K. Mahbub. August 2013. Incremental Certification of Cloud Services. In *Proc. of SECURWARE 2013*. Barcelona, Spain.

A. Kurmus, M. Gupta, R. Pletka, C. Cachin, and R. Haas. December 2011. A Comparison of Secure Multitenancy Architectures for Filesystem Storage Clouds. In *Proc. of ACM/IFIP/USENIX Middleware 2011*. Lisbon, Portugal.

U. Lang. November-December 2010. OpenPMF SCaaS: Authorization as a Service for Cloud & SOA Applications. In *Proc. of IEEE CloudCom 2010*. Indianapolis, IN, USA.

J.-H. Lee, M.-W. Park, J.-H. Eom, and T.-M. Chung. February 2011. Multi-level Intrusion Detection System and log management in Cloud Computing. In *Proc. of ICACT 2011*. Gangwon-Do, South Korea.

H. Li, Y. Dai, and B. Yang. 2011a. Identity-Based Cryptography for Cloud Security. *IACR Cryptology ePrint Archive* 2011 (2011), 169.

J. Li, B. Li, T. Wo, C. Hu, J. Huai, L. Liu, and K.P. Lam. 2011b. CyberGuarder: A virtualization security assurance architecture for green cloud computing. *Future Generation Computer Systems* 28, 2 (May 2011), 379–390.

M. Li, W. Zang, K. Bai, M. Yu, and P. Liu. December 2013. MyCloud: Supporting User-configured Privacy Protection in Cloud Computing. In *Proc. of ACSAC 2013*. New Orleans, LA, USA.

B. Libert and J.-J. Quisquater. 2011. Identity-Based Cryptosystems. In *Encyclopedia of Cryptography and Security*, H.C.A. van Tilborg and S. Jajodia (Eds.). Springer.

H.-Y. Lin and W.-G. Tzeng. 2012. A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding. *IEEE TPDS* 23, 6 (June 2012), 995–1003.

H. Liu. October 2010. A New Form of DOS Attack in a Cloud and Its Avoidance Mechanism. In *Proc. of ACM CCSW 2010*. Chicago, IL, USA.

X. Liu, Y. Xia, S. Jiang, F. Xia, and Y. Wang. July 2013. Hierarchical Attribute-Based Access Control with Authentication for Outsourced Data in Cloud Computing. In *Proc. of IEEE TrustCom 2013*. Melbourne, Australia.

F. Lombardi and R. Di Pietro. 2011. Secure virtualization for cloud computing. *Journal of Network and Computer Applications* 34, 4 (July 2011), 1113–1122.

F. Lombardi and R. Di Pietro. March 2010. Transparent Security for Cloud. In *Proc. of ACM SAC 2010*. Sierre, Switzerland.

W. Lu, X. Hu, S. Wang, and X. Li. 2014. A Multi-Criteria QoS-aware Trust Service Composition Algorithm in Cloud Computing Environments. *IJGDC* 7, 1 (2014), 77–88.

W. Luo, L. Xu, Z. Zhan, Q. Zheng, and S. Xu. 2014. Federated Cloud Security Architecture for Secure and Agile Clouds. In *High Performance Cloud Auditing and Applications*, K.J. Han, B.-Y. Choi, and S. Song (Eds.). Springer New York.

W. Ma, X. Li, Y. Shi, and Y. Guo. 2013. A Virtual Machine Cloning Approach Based on Trusted Computing. *TELKOMNIKA* 11, 11 (November 2013), 6935–6942.

I. MacNeil and X. Li. 2006. "Comply or Explain": market discipline and non-compliance with the Combined Code. *Corporate Governance: An International Review* 14, 5 (2006), 486–496.

K. Mahbub and G. Spanoudakis. 2007. Monitoring WS-Agreements: An Event CalculusBased Approach. In *Test and Analysis of Web Services*, L. Baresi and E. Di Nitto (Eds.). Springer Berlin Heidelberg, 265–306.

K. Mahbub and G. Spanoudakis. November 2004. A Framework for Requirents Monitoring of Service Based Systems. In *Proc. of ICSOC 2004*. New York, NY, USA.

R. Mahmood, N. Esfahani, T. Kacem, N. Mirzaei, S. Malek, and A. Stavrou. June 2012. A whitebox approach for automated security testing of Android applications on the cloud. In *Proc. of AST 2012*. Zurich, Switzerland.

S. Mansfield-Devine. 2008. Danger in the clouds. *Network Security* 2008, 12 (December 2008), 9–11.

D.C. Marinescu, A. Paya, J.P. Morrison, and P.D. Healy. 2013. An Auction-driven Self-organizing Cloud Delivery Model. *CoRR* abs/1312.2998 (2013).

M.L. Massie, B.N. Chun, and D.E. Culler. 2004. The ganglia distributed monitoring system: design, implementation, and experience. *Parallel Comput.* 30, 7 (July 2004), 817–840.

M. Massie, B. Li, B. Nicholes, V. Vuksan, R. Alexander, J. Buchbinder, F. Costa, A. Dean, D. Josephsen, P. Phaal, and D. Pocock. 2012. *Monitoring with Ganglia – Tracking Dynamic Host and Application Metrics at Scale*. O'Reilly Media.

M. McIntosh and P. Austel. November 2005. XML Signature Element Wrapping Attacks and Countermeasures. In *Proc. of SWS 2005*. Fairfax, VA, USA.

S. Mei, H. Ba, F. Tu, J. Ren, and Z. Wang. September 2013. TTP-ACE: A Trusted Third Party for Auditing in Cloud Environment. In *Proc. of ICSCTEA 2013*. September.

P. Mell and T. Grance. 2011. *The NIST Definition of Cloud Computing*. NIST SP-800-145, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

S. Meng and L. Liu. 2013. Enhanced Monitoring-as-a-Service for Effective Cloud Management. *IEEE TC* 62, 9 (September 2013), 1705–1720.

C. Modi, D. Patel, B. Borisaniya, A. Patel, and M. Rajarajan. 2013a. A Survey on Security Issues and Solutions at Different Layers of Cloud Computing. *Journal of Supercomputing* 63, 2 (February 2013).

C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan. 2013b. A survey of intrusion detection techniques in Cloud. *Journal of Network and Computer Applications* 36, 1 (June 2013), 42–57.

M. H. Mohamaddiah, A. Abdullah, S. Subramaniam, and M. Hussin. 2014. A Survey on Resource Allocation and Monitoring in Cloud Computing. *IJMLC* 4, 1 (February 2014).

A.T. Monfared and M.G. Jaatun. November-December 2011. Monitoring Intrusions and Security Breaches in Highly Distributed Cloud Environments. In *Proc. of IEEE CloudCom 2011*. Athens, Greece.

J. Moreno. 2010. *A Testing Framework for Cloud Storage Systems*. Master Thesis – ETH Zürich, http://e-collection.library.ethz.ch/eserv/eth:1987/eth-1987-01.pdf.

T. Morris. 2011. Trusted Platform Module. In *Encyclopedia of Cryptography and Security*, H.C.A. van Tilborg and S. Jajodia (Eds.). Springer.

O. Moser, F. Rosenberg, and S. Dustdar. April 2008. Non-intrusive Monitoring and Service Adaptation for WS-BPEL. In *Proc. of WWW 2008*. Beijing, China.

H. Mouratidis, S. Islam, C. Kalloniatis, and S. Gritzalis. 2013. A framework to support selection of cloud providers based on security and privacy requirements. *JSS* 86, 9 (March 2013), 2276–2293.

A. Muñoz and A. Maña. June 2013. Bridging the GAP between Software Certification and Trusted Computing for Securing Cloud Computing. In *Proc. of IEEE SERVICES 2013*. Santa Clara, CA, USA.

I. Muttik and C. Barton. 2009. Cloud security technologies. *Information Security Technical Report* 14, 1 (2009), 1–6.

M. Nabeel, N. Shang, and E. Bertino. 2013. Privacy Preserving Policy-Based Content Sharing in Public Clouds. *IEEE TKDE* 25, 11 (November 2013), 2602–2614.

Nagios. 2014. *Cloud Computing*. http://www.nagios.com/solutions/cloud-computing.

Network of Excellence on Engineering Secure Future Internet Software Services and Systems 2010. *Network of Excellence on Engineering Secure Future Internet Software Services and Systems*. http://www.nessos-project.eu/.

J. Ni, Y. Yu, Y. Mu, and Q. Xia. 2014. On the Security of an Efficient Dynamic Auditing Protocol in Cloud Storage. *IEEE TPDS* (2014).

K. Okamura and Y. Oyama. March 2010. Load-based Covert Channels Between Xen Virtual Machines. In *Proc. of ACM SAC 2010*. Sierre, Switzerland.

M. Okuhara, T. Shiozaki, and T. Suzuki. 2010. Security Architectures for Cloud Computing. *Fujitsu scientific and technical journal* 46, 4 (October 2010), 397–402.

OpenStack Open Source Cloud Computing Software 2015. *OpenStack Open Source Cloud Computing Software*. https://www.openstack.org/.

N. Paladi, C. Gehrmann, and F. Morenius. March 2013. *State of The Art and Hot Aspects in Cloud Data Storage Security*. SICS technical report T2013:01.

M.P. Papazoglou, V. Andrikopoulos, and S. Benbernou. 2011. Managing Evolving Services. *IEEE Software* 28, 3 (May-June 2011), 49–55.

S. Paquette, P.T. Jaeger, and S.C. Wilson. 2010. Identifying the security risks associated with governmental use of cloud computing. *Government Information Quarterly* 27, 3 (April 2010), 245–253.

K.-W. Park, J. Han, J. Chung, and K.H. Park. 2013. THEMIS: A Mutually Verifiable Billing System for the Cloud Computing Environment. *IEEE TSC* 6, 3 (July-September 2013), 300–313.

T. Parveen and S. Tilley. April 2010. When to Migrate Software Testing to the Cloud?. In *Proc of ICSTW 2010*. Paris, France.

A. Patel, M. Taghavi, K. Bakhtiyari, and J. Celestino JúNior. 2013. An Intrusion Detection and Prevention System in Cloud Computing: A Systematic Review. *Journal of Network and Computer Applications* 36, 1 (January 2013), 25–41.

E. Pattuk, M. Kantarcioglu, V. Khadilkar, H. Ulusoy, and S. Mehrotra. June 2013. BigSecret: A Secure Data Management Framework for Key-Value Stores. In *Proc. of IEEE CLOUD 2013*. Santa Clara, CA, USA.

M. Pearce, S. Zeadally, and R. Hunt. 2013. Virtualization: Issues, Security Threats, and Solutions. *ACM CSUR* 45, 2 (February 2013), 17:1–17:39.

S. Pearson. 2011. Toward Accountability in the Cloud. *IEEE Internet Computing* 15, 4 (2011), 64–69.

S. Pearson. 2013. Privacy, Security and Trust in Cloud Computing. In *Privacy and Security for Cloud Computing*, S. Pearson and G. Yee (Eds.). Springer London, 3–42.

S. Pearson and A. Benameur. November-December 2010. Privacy, Security and Trust Issues Arising from Cloud Computing. In *Proc. of IEEE CloudCom 2010*. Indianapolis, IN, USA.

S. Pearson, Y. Shen, and M. Mowbray. December 2009. A Privacy Manager for Cloud Computing. In *Proc. of CloudCom 2009*. Beijing, China.

D. Perez-Botero, J. Szefer, and R.B. Lee. May 2013. Characterizing Hypervisor Vulnerabilities in Cloud Computing Servers. In *Proc. of ASIACCS-SCC 2013*. Hangzhou, China.

G. Peterson. 2010. Don't Trust. And Verify: A Security Architecture Stack for the Cloud. *IEEE Security & Privacy* 8, 5 (September-October 2010), 83–86.

C. Pham, D. Chen, Z. Kalbarczyk, and R.K. Iyer. June 2011. CloudVal: A framework for validation of virtualization environment in cloud infrastructure. In *Proc of IEEE/IFIP DSN 2011*. Hong Kong, China.

Policy and Security Configuration Management 2010. *Policy and Security Configuration Management*. http://www.posecco.eu/.

G. Porter. 2013. *Cloud Service Provider Methods for Managing Insider Threats: Analysis Phase I*. Technical Note, CMU/SEI-2013-TN-020.

B. Preneel. 2011. MAC Algorithms. In *Encyclopedia of Cryptography and Security*, H.C.A. van Tilborg and S. Jajodia (Eds.). Springer.

B. Qin, H. Wang, Q. Wu, J. Liu, and J. Domingo-Ferrer. 2013. Simultaneous authentication and secrecy in identity-based data upload to cloud. *Cluster Computing* 16, 4 (April 2013), 845–859.

M.N. Rajkumar, V.V. Kumar, and R. Sivaramakrishnan. 2013. Efficient Integrity Auditing Services for Cloud Computing Using Raptor Codes. In *Proc. of ACM RACS 2013*. Montreal, QC, Canada.

J. Rao, Y. Wei, J. Gong, and C.-Z. Xu. 2013. QoS Guarantees and Service Differentiation for Dynamic Cloud Applications. *IEEE TNSM* 10, 1 (March 2013), 43–55.

H. Rasheed. 2013. Data and infrastructure security auditing in cloud computing environments. *IJIM* (December 2013).

M. Raykova, H. Zhao, and S.M. Bellovin. February-March 2012. Privacy Enhanced Access Control for Outsourced Data Sharing. In *Proc. of FC 2012*. Bonaire.

K. Ren, C. Wang, and Q. Wang. 2012. Security Challenges for the Public Cloud. *IEEE Internet Computing* 16, 1 (January-February 2012), 69–73.

Resources and Services Virtualization without Barriers 2008. *Resources and Services Virtualization without Barriers*. http://www.reservoir-fp7.eu/.

Risk Assessment Techniques for Off-line and On-line Security Evaluation of Cloud Computing 2013. *Risk Assessment Techniques for Off-line and On-line Security Evaluation of Cloud Computing*. http://www.nsf.gov/awardsearch/showAward?AWD_ID=1332035&HistoricalAwards=false.

T. Ristenpart, E. Tromer, H. Shacham, and S. Savage. November 2009. Hey, You, Get off of My Cloud: Exploring Information Leakage in Third-party Compute Clouds. In *Proc. of ACM CCS 2009*. Chicago, IL, USA.

L.M. Riungu, O. Taipale, and K. Smolander. November-December 2010. Research Issues for Software Testing in the Cloud. In *Proc. of IEEE CloudCom 2010*. Indianapolis, IN, USA.

F. Rocha and M. Correia. June 2011. Lucy in the sky without diamonds: Stealing confidential data in the cloud. In *Proc. of IEEE/IFIP DSN-W 2011*. Hong Kong, China.

L. Rodero-Merino, L.M. Vaquero, E. Caron, A. Muresan, and F. Desprez. 2012. Building safe PaaS clouds: A survey on security in multitenant software platforms. *Computers & Security* 31, 1 (February 2012), 96–108.

C. Rong, S.T. Nguyen, and M.G. Jaatun. 2013. Beyond lightning: A survey on security challenges in cloud computing. *Computers & Electrical Engineering* 39, 1 (May 2013), 47–54.

S. Ruj, M. Stojmenovic, and A. Nayak. 2014. Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds. *IEEE TPDS* 25, 2 (February 2014), 384–394.

M.D. Ryan. 2013. Cloud computing security: The scientific challenge, and a survey of solutions. *JSS* 86, 9 (February 2013), 2263–2268.

S.H. Ryu, F. Casati, H. Skogsrud, B. Betanallah, and R. Saint-Paul. 2008. Supporting the Dynamic Evolution of Web Service Protocols in Service-Oriented Architectures. *ACM TWEB* 2, 2 (April 2008), 13:1–13:46.

S. Sakr and A. Liu. June 2012. SLA-Based and Consumer-centric Dynamic Provisioning for Cloud Databases. In *Proc. of IEEE CLOUD 2012*. Honolulu, HI, Hawaii.

M. Salifu, Yijun Yu, and B. Nuseibeh. October 2007. Specifying Monitoring and Switching Problems in Context. In *Proc. of IEEE RE 2007*. New Delhi, India.

N. Santos, R. Rodrigues, K.P. Gummadi, and S. Saroiu. August 2012. Policy-sealed data: A new abstraction for building trusted cloud services. In *Proc. of USENIX Security Symposium 2012*. Bellevue, WA, USA.

P. Saripalli and B. Walters. 2010. QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security. In *Proc. of IEEE CLOUD 2010*. Miami, FL, USA.

M. Schumacher, E.B. Fernandez, D. Hybertson, F. Buschmann, and P. Sommerlad. 2006. *Security Patterns: Integrating security and systems engineering*. Wiley.

Secure and Privacy-assured Data Service Outsourcing in Cloud Computing 2012. *Secure and Privacy-assured Data Service Outsourcing in Cloud Computing*. http://www.nsf.gov/awardsearch/showAward?AWD_ID=1262277&HistoricalAwards=false.

Secure Data-Intensive Computing on Hybrid Clouds 2012. *Secure Data-Intensive Computing on Hybrid Clouds*. http://www.nsf.gov/awardsearch/showAward?AWD_ID=1223495&HistoricalAwards=false.

Secure Provision and Consumption in the Internet of Services 2010. *Secure Provision and Consumption in the Internet of Services*. http://www.spacios.eu/.

Secure Provisioning of Cloud Services based on SLA management 2013. *Secure Provisioning of Cloud Services based on SLA management*. http://specs-project.eu/.

J. Sedayao, S. Su, X. Ma, M. Jiang, and K. Miao. December 2009. A Simple Technique for Securing Data at Rest Stored in a Computing Cloud. In *Proc. of CloudCom 2009*. Beijing, China.

SEI 2011. Securing Web Services for Army SOA. (2011). http://www.sei.cmu.edu/solutions/softwaredev/securing-web-services.cfm.

S. Sengupta, V. Kaulgud, and V.S. Sharma. July 2011. Cloud Computing Security–Trends and Research Directions. In *Proc. of IEEE SERVICES 2011*. Washington, VA, USA.

J. Shao, H. Wei, Q. Wang, and H. Mei. July 2010. A Runtime Model Based Monitoring Approach for Cloud. In *Proc. of IEEE CLOUD 2010*. Miami, FL, USA.

S. Shetty. June-July 2013. Auditing and Analysis of Network Traffic in Cloud Environment. In *Proc. of IEEE SERVICES 2013*. Santa Clara, CA, USA.

A. Shraer, C. Cachin, A. Cidon, I. Keidar, Y. Michalevsky, and D. Shaket. October 2010. Venus: Verification for Untrusted Cloud Storage. In *Proc. of ACM CCSW 2010*. Chicago, IL, USA.

J. Simmonds, Y. Gan, M. Chechik, S. Nejati, B. O'Farrell, E. Litani, and J. Waterhouse. 2009. Runtime Monitoring of Web Service Conversations. *IEEE TSC* 2, 3 (July–September 2009), 223–244.

M. Singhal, S. Chandrasekhar, T. Ge, R. Sandhu, R. Krishnan, G.-J. Ahn, and E. Bertino. 2013. Collaboration in multicloud computing environments: Framework and security issues. *Computer* 46, 2 (February 2013), 76–84.

J. Somorovsky, M. Heiderich, M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono. 2011. All Your Clouds Are Belong to Us: Security Analysis of Cloud Management Interfaces. In *Proc. of ACM CCSW 2011*. Chicago, IL, USA.

Z. Song, J. Molina, S. Lee, H. Lee, S. Kotani, and R. Masuoka. 2009. TrustCube: An Infrastructure that Builds Trust in Client. In *Future of Trust in Computing*, D. Gawrock, H. Reimer, A.-R. Sadeghi, and C. Vishik (Eds.). Vieweg+Teubner, 68–79.

G. Spanoudakis, E. Damiani, and A. Maña. October 2012. Certifying Services in Cloud: The Case for a Hybrid, Incremental and Multi-layer Approach. In *Proc. of IEEE HASE 2012*. Omaha, NE, USA.

M.K. Srinivasan, K. Sarukesi, P. Rodrigues, M.S. Manoj, and P. Revathy. August 2012. State-of-the-art Cloud Computing Security Taxonomies: A Classification of Security Challenges in the Present Cloud Computing Environment. In *Proc. of ICACCI 2012*. Chennai, India.

M. Srivatsa and A. Iyengar. 2011. Application-Level Denial of Service. In *Encyclopedia of Cryptography and Security*, H.C.A. van Tilborg and S. Jajodia (Eds.). Springer.

O. Starov and S. Vilkomir. May 2013. Integrated TaaS platform for mobile development: Architecture solutions. In *Proc. of AST 2013*. San Francisco, CA, USA.

E. Stefanov, M. van Dijk, A. Juels, and A. Oprea. December 2012. Iris: A Scalable Cloud File System with Efficient Integrity Checks. In *Proc. of ACSAC 2012*. Orlando, FL, USA.

S.J. Stolfo, M.B. Salem, and A.D. Keromytis. May 2012. Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud. In *Proc. of IEEE SPW 2012*. San Francisco, CA, USA.

S. Subashini and V. Kavitha. 2011. A Survey on Security Issues in Service Delivery Models of Cloud Computing. *Journal of Network and Computer Applications* 34, 1 (January 2011), 1–11.

A. Sulistio and C. Reich. September 2013. Towards a Self-protecting Cloud. In *Proc. of OTM 2013*. Graz, Austria.

S. Sundareswaran, A. C. Squicciarini, and D. Lin. 2012. Ensuring Distributed Accountability for Data Sharing in the Cloud. *IEEE TDSC* 9, 4 (July 2012), 556–568.

A. Sunyaev and S. Schneider. 2013. Cloud Services Certification. *CACM* 56, 2 (February 2013), 33–36.

J. Szefer and R.B. Lee. 2014. Hardware-Enhanced Security for Cloud Computing. In *Secure Cloud Computing*, S. Jajodia, K. Kant, P. Samarati, V. Swarup, and C. Wang (Eds.). Springer.

H. Takabi and J.B.D. Joshi. January 2012. Policy Management as a Service: An Approach to Manage Policy Heterogeneity in Cloud Computing Environment. In *Proc. of HICSS 2012*. Maui, HI, Hawaii.

H. Takabi, J.B.D. Joshi, and Gail-Joon Ahn. 2010b. Security and Privacy Challenges in Cloud Computing Environments. *IEEE Security & Privacy* 8, 6 (November-December 2010), 24–31.

H. Takabi, J.B.D. Joshi, and G.-J. Ahn. July 2010a. SecureCloud: Towards a Comprehensive Security Framework for Cloud Computing Environments. In *Proc. of IEEE COMPSACW 2010*. Seoul, South Korea.

T. Takahashi, G. Blanc, Y. Kadobayashi, D. Fall, H. Hazeyama, and S. Matsuo. April 2012. Enabling secure multitenancy in cloud computing: Challenges and approaches. In *Proc. of BCFIC 2012*. Vilnius, Lithuania.

Y. Tang, P. P. C. Lee, J. C. S. Lui, and R. Perlman. 2012. Secure Overlay Cloud Storage with Access Control and Assured Deletion. *IEEE TDSC* 9, 6 (November 2012), 903–916.

D. Thebeau II, B. Reidy, R. Valerdi, A. Gudagi, H. Kurra, Y. Al-Nashif, S. Hariri, and F. Sheldon. March 2014. Improving Cyber Resiliency of Cloud Application Services by Applying Software Behavior Encryption (SBE). In *Proc. of CSER 2014*. Redondo Beach, CA, USA.

Trend Micro. April 2013. *Best Practices for Security and Compliance with Amazon Web Services*. https://reinvent.awsevents.com/files/TrendMicro_Whitepaper.pdf.

H.-L. Truong_c and T. Fahringer. 2004. SCALEA-G: A Unified Monitoring and Performance Analysis System for the Grid. *Scientific Programming* 12, 4 (December 2004), 225–237.

H.-Y. Tsai, M. Siebenhaar, A. Miede, Y.-L. Huang, and R. Steinmetz. 2012. Threat as a Service? Virtualization's Impact on Cloud Security. *IT Professional* 14, 1 (January-February 2012), 32–37.

W.-T. Tsai, P. Zhong, J. Balasooriya, Y. Chen, X. Bai, and J. Elston. June-July 2011. An Approach for Service Composition and Testing for Cloud Computing. In *Proc. of ISADS 2011*. Kobe, Japan.

P.K. Tysowski and M.A. Hasan. 2013. Hybrid Attribute- and Re-Encryption-Based Key Management for Secure and Scalable Mobile Applications in Clouds. *IEEE TCC* 1, 2 (July 2013), 172–186.

M. van Dijk, A. Juels, A. Oprea, R.L. Rivest, E. Stefanov, and N. Triandopoulos. October 2012. Hourglass Schemes: How to Prove That Cloud Files Are Encrypted. In *Proc. of ACM CCS 2012*. Raleigh, NC, USA.

E. van Veenendaal. October 2012. *Standard glossary of terms used in Software Testing*. International Software Testing Qualifications Board (ISTQB). http://www.istqb.org/downloads/finish/20/101.html.

L.M. Vaquero, L. Rodero-Merino, and D. Moran. 2011. Locking the Sky: A Survey on IaaS Cloud Security. *Computing* 91, 1 (January 2011), 93–118.

M. Velten and F. Stumpf. November 2013. Secure and Privacy-Aware Multiplexing of Hardware-Protected TPM Integrity Measurements among Virtual Machines. In *Proc. of ICISC 2012*. Seoul, South Korea.

Z. Wan, J. Liu, and R.-H. Deng. 2012. HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing. *IEEE TIFS* 7, 2 (April 2012), 743–754.

B. Wang, S.S.M. Chow, M. Li, and H. Li. July 2013a. Storing Shared Data on the Cloud via Security-Mediator. In *Proc. of IEEE ICDCS 2013*. Philadelphia, PA, USA.

B. Wang, B. Li, and H. Li. 2014. Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud. *IEEE TCC* (2014).

B. Wang, B. Li, and H. Li. April 2013. Public auditing for shared data with efficient user revocation in the cloud. In *Proc. of IEEE INFOCOM 2013*. Turin, Italy.

C. Wang, N. Cao, K. Ren, and W. Lou. 2012. Enabling Secure and Efficient Ranked Keyword Search over Outsourced Cloud Data. *IEEE TPDS* 23, 8 (August 2012), 1467–1479.

C. Wang, S.S.M. Chow, Q. Wang, K. Ren, and W. Lou. 2013b. Privacy-Preserving Public Auditing for Secure Cloud Storage. *IEEE TC* 62, 2 (February 2013), 362–375.

C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou. 2012. Toward Secure and Dependable Storage Services in Cloud Computing. *IEEE TSC* 5, 2 (April 2012), 220–232.

C. Wang, Q. Wang, K. Ren, and W. Lou. March 2010. Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing. In *Proc. of IEEE INFOCOM 2010*. San Diego, CA, USA.

M. Wang, V. Holub, T. Parsons, J. Murphy, and P. O'Sullivan. March 2010. Scalable Run-Time Correlation Engine for Monitoring in a Cloud Computing Environment. In *Proc. of IEEE ECBS 2010*. Oxford, UK.

Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li. 2011. Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing. *IEEE TPDS* 22, 5 (May 2011), 847–859.

J. Wei, C. Pu, C.V. Rozas, A. Rajan, and F. Zhu. November-December 2013. Modeling the Runtime Integrity of Cloud Servers: A Scoped Invariant Perspective. In *Proc. of IEEE CloudCom 2010*. Indianapolis, IN, USA.

L. Wei and M.K. Reiter. September 2012. Third-Party Private DFA Evaluation on Encrypted Files in the Cloud. In *Proc. of ESORICS 2012*. Pisa, Italy.

L. Wei and M.K. Reiter. September 2013. Ensuring File Authenticity in Private DFA Evaluation on Encrypted Files in the Cloud. In *Proc. of ESORICS 2013*. Egham, UK.

L. Wei, H. Zhu, Z. Cao, X. Dong, W. Jia, Y. Chen, and A.V. Vasilakos. April 2014. Security and privacy for storage and computation in cloud computing. *Information Sciences* 258 (April April 2014), 371–386.

P. Wieder, J.M. Butler, W. Theilmann, and R. Yahyapour. 2011. *Service Level Agreements for Cloud Computing*. Springer.

Z. Xiao and Y. Xiao. 2013. Security and Privacy in Cloud Computing. *IEEE Communications Surveys & Tutorials* 15, 2 (April-June 2013), 843–859.

T. Xing, D. Huang, L. Xu, C.-J. Chung, and P. Khatkar. March 2013. SnortFlow: A OpenFlow-Based Intrusion Prevention System in Cloud Environment. In *Proc. of GENI GREE 2012*. New Utah, UT, USA.

L. Xu, X. Cao, Y. Zhang, and W. Wu. 2013a. Software Service Signature (S3) for authentication in cloud computing. *Cluster Computing* 16, 4 (December 2013), 905–914.

Z. Xu, C. Wang, Q. Wang, K. Ren, and L. Wang. April 2013b. Proof-carrying cloud computation: The case of convex optimization. In *Proc. of IEEE INFOCOM 2013*. Turin, Italy.

K. Yang and X. Jia. 2013. An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing. *IEEE TPDS* 24, 9 (September 2013), 1717–1726.

K. Yang, X. Jia, K. Ren, and B. Zhang. April 2013. DAC-MACS: Effective data access control for multi-authority cloud storage systems. In *Proc. of IEEE INFOCOM 2013*. Turin, Italy.

L. Ye, H. Zhang, J. Shi, and X. Du. December 2012. Verifying cloud Service Level Agreement. In *Proc. of IEEE GLOBECOM 2012*. Anaheim, CA, USA.

Y.A. Younis, M. Merabti, and K. Kifayat. 2013. *Secure Cloud Computing for Critical Infrastructure A Survey*. http://www.cms.livjm.ac.uk/pgnet2013/proceedings/papers/1569764399.pdf.

J. Yu, P. Lu, Y. Zhu, G. Xue, and M. Li. 2013a. Toward Secure Multikeyword Top-k Retrieval over Encrypted Cloud Data. *IEEE TDSC* 10, 4 (July 2013), 239–250.

L. Yu, W.-T. Tsai, X. Chen, L. Liu, Y. Zhao, L. Tang, and W. Zhao. June 2010a. Testing as a Service over Cloud. In *Proc. of IEEE SOSE 2010*. Nanjing, China.

S. Yu, Y. Tian, S. Guo, and D. Wu. 2013b. Can We Beat DDoS Attacks in Clouds? *IEEE TPDS* (July 2013).

S. Yu, C. Wang, K. Ren, and W. Lou. March 2010b. Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing. In *Proc. of IEEE INFOCOM 2010*. San Diego, CA, USA.

S. Zawoad, A.K. Dutta, and R. Hasan. May 2013. SecLaaS: Secure Logging-as-a-service for Cloud Forensics. In *Proc. of ACM ASIACCS 2013*. Hangzhou, China.

P. Zech. March 2011. Risk-Based Security Testing in Cloud Computing Environments. In *Proc. of IEEE ICST 2011*. Berlin, Germany.

Y. Zhang, A. Juels, M.K. Reiter, and T. Ristenpart. October 2012. Cross-VM Side Channels and Their Use to Extract Private Keys. In *Proc. of ACM CCS 2012*.

Y. Zhang and M.K. Reiter. November 2013. Düppel: Retrofitting Commodity Operating Systems to Mitigate Cache Side Channels in the Cloud. In *Proc. of ACM CCS 2013*. Berlin, Germany.

L. Zhao, Y. Ren, M. Li, and K. Sakurai. 2012. Flexible service selection with user-specific QoS support in service-oriented architecture. *Journal of Network and Computer Applications* 35, 3 (March 2012), 962–973.

M. Zhou, R. Zhang, W. Xie, W. Qian, and A. Zhou. November 2010. Security and Privacy in Cloud Computing: A Survey. In *Proc. of SKG 2010*. Ningbo, China.

Y. Zhu, G.-J. Ahn, H. Hu, S. S. Yau, H. G. An, and C.-J. Hu. 2013. Dynamic Audit Services for Outsourced Storages in Clouds. *IEEE TSC* 6, 2 (April 2013), 227–238.

Y. Zhu, H. Hu, G.-J. Ahn, D. Huang, and S. Wang. March 2012. Towards temporal access control in cloud computing. In *Proc. of IEEE INFOCOM 2012*. Orlando, FL, USA.

D. Zissis and D. Lekkas. 2012. Addressing Cloud Computing Security Issues. *Future Generation Computer Systems* 28, 3 (March 2012), 583–592.

D. Zou, W. Zhang, W. Qiang, G. Xiang, L.T. Yang, H. Jin, and K. Hu. 2013. Design and implementation of a trusted monitoring framework for cloud platforms. *Future Generation Computer Systems* 29, 8 (October 2013), 2092–2102.

A. MISCELLANEA

A.1. Vulnerabilities, threats, attacks, and risk evaluation

In this section, we extend the discussion in Section 3 and provide an overview of vulnerabilities, threats, and attacks that insist on more than one attack surface in Section 2, without a preferred surface for a successful exploit.

Paquette et al. [Paquette et al. 2010] analyze the risks faced by a governmental institution moving to the cloud and highlight the need for risk management. Saripalli and Walters [Saripalli and Walters 2010] present *QUIRC*, a quantitative risk and impact assessment framework that permits to assess security risks in cloud computing platforms, mainly considering confidentiality, integrity, and availability. QUIRC enables customer to compare the robustness of cloud providers' offerings. Grobauer et al. [Grobauer et al. 2011] study cloud computing vulnerabilities and their impact on cloud. They also propose some indicators of cloud-specific vulnerabilities on the basis of risk factors. Dahbur et al. [Dahbur et al. 2011] present a survey on risks, threats, and vulnerabilities in cloud computing. In addition to attempting a novel definition of the concepts of risks, threats, and vulnerabilities in the cloud, it presents some real world examples of attacks: *i)* using IaaS to host crimeware, where cloud resources are used as startup points for attacks that target both cloud and external applications and resources; *ii)* virtualization attacks, where tenant-on-tenant attacks in general, and the blue pill rootkit[3] in particular, are described; *iii)* cloud computing outage and data loss, where some successful attacks on providers like Salesforce.com and Rackspace are presented. Booth et al. [Booth et al. 2013] present a different classification of cloud security, which is built around attack strategies and corresponding defenses. The paper classifies attacks and defenses using the following categories: denial of service, breach of confidentiality, data availability and integrity, data confidentiality. In the discussion, different attacks belonging to tenant-on-tenant and provider-on-tenant attack surfaces are described.

A.2. Cloud security

In this section, we extend the discussion in Section 4 and present a summary of techniques selected on the basis of criteria in Section 2.1 and spanning more than one of the cloud security macro-areas identified in Section 2.2.

Okuhara et al. [Okuhara et al. 2010] propose *Trusted-Service Platform*, an access control, authentication, and identification platform for cloud services. Takabi et al. [Takabi et al. 2010a] present *SecureCloud*, a security framework for the cloud that consists of different modules for managing security and trust. In particular, SecureCloud focuses on identity management, access control, policy integration among multiple clouds, trust management between different clouds and between a cloud and its users, secure service composition and integration, and semantic heterogeneity among policies from different clouds. An interesting line of research is the one providing cloud-specific version of general-purpose security patterns [Schumacher et al. 2006]. Peterson [Peterson 2010] presents a security stack for the cloud that builds on four patterns: *i)* gateway as the defensive structure to limit attack surface and enforce policies, *ii)* monitor to collect and analyze cloud events, *iii)* security token service to issue, validate, and exchange tokens, *iv)* policy enforcement point/policy decision point to define, evaluate, and enforce policies. Patterns are based on different security techniques, including access control, encryption, and authentication. Li et al. [Li et al. 2011b]

[3]The blue pill rootkit forces an operating system that believes to run on a real system, to execute on a virtual version of it. It traps the running operating system by deploying a thin hypervisor and virtualizing the rest of the machine under it. All communications can then be intercepted by the hypervisor, which can further send fake replies.

present a virtualization security assurance architecture, called *CyberGuarder*, which addresses security problems in the context of green cloud computing. CyberGuarder includes a virtual machine security service, a virtual network security service, and a policy-based trust management service. Jhawar et al. [Jhawar et al. 2012] propose a novel cloud resource allocation algorithm that takes into account security (and also availability and reliability) requirements. Their framework allows providers to define regulations on the allocation of their resources and customers to express constraints on the distribution of their virtual machines (e.g., geographical placement). Bernsmed et al. [Bernsmed et al. 2012] present a survey of security challenges and solutions for federated clouds, describe some approaches to secure cloud federations, and discuss future research directions. Singhal et al. [Singhal et al. 2013] discuss the problem of addressing security, trust, privacy, and policy evaluation in the context of collaboration in multicloud computing environments. They propose a proxy multicloud computing framework supporting dynamic and runtime collaborations between cloud-based services. Zhang and Reiter [Zhang and Reiter 2013] present *Düppel*, a system enabling tenant virtual machines to defend themselves from cache-based side-channel attacks in public clouds. Their approach defends cloud tenants by automatically injecting noise into the timings that an attacker observes from caches. Xu et al. [Xu et al. 2013b] introduce an efficient integrity verification mechanism to secure computations outsourced to the cloud. The proposed approach considers the outsourcing of the convex optimization problem and analyzes mechanisms based on application-specific techniques for efficient integrity verification. Wei et al. [Wei et al. 2013] propose a technique based on scoped invariants to evaluate the integrity of cloud servers and software. The authors provide a case study of the application of the proposed approach on the Xen Virtual Machine Manager. De Capitani di Vimercati et al. [De Capitani di Vimercati et al. 2014] compare different solutions to protect outsourced data and enforce fine-grained and selective access, and evaluate privacy issues that might arise. Some work has been also done towards the development of resilient cloud services [Dsouza et al. 2013; Thebeau II et al. 2014]. The solution in [Dsouza et al. 2013] is based on dynamic data driven application system and moving target defence strategies to support resilient cloud service development. The proposed approach makes the system execution environment target of an attack dynamic, complicating exploits of vulnerabilities by attackers. It is based on software behavior encryption, replication, diversity, and automated checkpointing and recovery. In the same scenario, Thebeau II et al. [Thebeau II et al. 2014] complement the work in [Dsouza et al. 2013] by providing a solution to define and measure cyber resiliency of cloud applications. First they describe the components of resiliency: attack surface, survivability, integrity, availability, and confidentiality. Then they discuss their measurement and aggregation through a worked-out example.

B. SUMMARY OF REVIEWED PAPERS

Tables V and VI present a summary of reviewed papers according to the *when*, *where*, *what*, *how* methodology in Section 2. In particular, each work has been categorized according to *i)* the year and corresponding quarter in which it has been published (when),[4] *ii)* the attack surface targeted by the given solution (where),[5] *iii)* the properties considered by the proposed solution (what), *iv)* the security/assurance techniques at the basis of the proposed solution (how). In Tables V and VI, ✓ means that a specific

[4]We note that the year is presented in the first column of Tables V and VI within the references.

[5]We note that the attack surfaces (application-level, tenant-on-tenant, provider-on-tenant/tenant-on-provider) refer to the set of resources owned by the corresponding actors (users, tenants, providers) and target of the surveyed approaches.

Table IV. Legenda for Tables V and VI

1QT=1^{st} quarter of the year	PC=Confidentiality	AC=Access Control
2QT=2^{nd} quarter of the year	PI=Integrity	AU=Authentication
3QT=3^{rd} quarter of the year	PA=Availability	TC=Trusted Computing
4QT=4^{th} quarter of the year	PU=Authenticity	M=Monitoring
AL=Application Level	PP=Privacy	AD=Audit/Compliance
TT=Tenant-on-Tenant	E=Encryption	SLA=Service Level Agreement
PT=Provider-on-Tenant	S=Signature	C=Certification
Tenant-on-Provider	I=IDS/IPS	T=Testing

Table V. Classification based on *when*, *where*, *what*, *how* dimensions

Reference (Year)	When				Where			What					How									
	1Q	2Q	3Q	4Q	AL	TT	PT	PC	PI	PA	PU	PP	E	S	I	AC	AU	TC	M	AD	SLA	C	T
[Aceto et al. 2013]	×	✓	×	×	✓	✓	✓	×	×	×	×	×	×	×	×	×	×	×	✓	×	×	×	×
[Ahmed et al. 2012]	×	×	✓	×	×	✓	×	✓	✓	✓	×	×	✓	×	×	×	×	×	×	×	×	×	×
[Alhamazani et al. 2013]	×	×	×	×	✓	✓	✓	×	×	×	×	×	×	×	×	×	×	×	✓	×	×	×	×
[Almulla and Yeun 2010]	✓	✓	×	×	✓	×	×	✓	×	×	×	×	×	✓	×	×	∼	×	×	×	×	×	×
[Anisetti et al. 2014]	×	×	✓	×	✓	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	✓	×	×
[Attasena et al. 2013]	×	×	✓	×	×	✓	✓	×	✓	✓	×	✓	✓	✓	×	×	×	×	×	×	×	×	×
[Bacon et al. 2014]	×	×	×	×	✓	✓	×	✓	×	×	×	×	×	×	×	✓	×	×	×	∼	×	×	×
[Bai et al. 2011]	×	×	×	✓	✓	✓	✓	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	✓
[Bai et al. 2013]	×	✓	×	×	✓	✓	✓	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	✓
[Barsoum and Hasan 2013]	×	×	×	✓	×	×	✓	✓	✓	×	✓	×	✓	×	×	✓	✓	×	×	×	×	×	×
[Benali et al. 2010]	×	×	✓	×	✓	×	×	×	×	×	×	✓	×	×	✓	×	×	×	×	×	×	×	×
[Bennani et al. 2010]	×	×	✓	×	✓	✓	✓	✓	×	×	×	×	✓	×	×	×	×	×	×	×	×	×	×
[Bernsmed et al. 2011]	×	×	✓	×	✓	×	×	✓	✓	✓	✓	✓	×	×	×	×	×	×	∼	×	✓	×	×
[Bernsmed et al. 2012]	×	×	×	✓	✓	✓	×	✓	✓	×	×	×	✓	×	×	×	×	✓	×	×	✓	×	×
[Bertholon et al. 2011]	×	×	✓	×	×	✓	×	∼	✓	×	×	×	∼	∼	×	×	×	✓	×	×	×	✓	×
[Birgisson et al. 2014]	✓	×	×	×	✓	×	×	✓	×	×	×	✓	∼	×	×	✓	×	×	×	×	×	×	×
[Birnbaum et al. 2013]	×	✓	✓	×	×	✓	×	✓	✓	×	✓	×	×	×	×	×	×	∼	✓	×	×	×	×
[Bleikertz et al. 2013]	×	✓	×	×	×	✓	✓	✓	×	×	×	✓	✓	×	×	×	×	✓	×	×	×	×	×
[Bleikertz et al. 2012]	×	✓	×	×	×	×	✓	×	✓	×	×	✓	×	×	×	✓	×	×	×	×	×	×	×
[Boampong and Wahsheh 2012]	✓	×	×	×	✓	✓	×	✓	✓	×	✓	×	×	×	×	×	×	✓	×	×	×	×	×
[Bowers et al. 2009]	×	×	×	✓	×	✓	×	✓	✓	✓	×	×	✓	×	×	×	×	×	×	×	×	×	×
[Candea et al. 2010]	×	✓	×	×	✓	×	×	✓	✓	✓	✓	✓	×	×	×	×	×	×	×	×	×	×	✓
[Casalicchio and Silvestri 2013]	✓	×	×	×	×	✓	×	×	×	×	×	×	×	×	×	×	×	×	×	×	✓	×	×
[Chan et al. 2009]	×	×	×	✓	✓	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	✓
[Chauhan et al. 2013]	×	×	×	✓	✓	×	✓	✓	✓	✓	✓	✓	×	×	×	×	×	×	✓	×	×	×	×
[Chonka et al. 2011]	×	×	✓	×	✓	✓	×	×	×	✓	×	×	×	×	✓	×	×	×	×	×	×	×	×
[Chow et al. 2012]	×	×	×	×	×	✓	✓	✓	×	×	✓	✓	✓	✓	×	×	×	×	×	×	×	×	×
[Christodorescu et al. 2009]	×	×	×	✓	×	✓	×	×	✓	×	×	×	×	×	✓	×	×	×	∼	×	×	×	×
[Chu et al. 2014]	✓	×	×	×	×	✓	✓	✓	×	×	✓	×	✓	×	×	×	∼	×	×	×	×	×	×
[Cimato et al. 2013]	×	✓	✓	×	✓	✓	✓	×	×	×	×	×	×	×	×	×	×	∼	∼	×	×	✓	∼
[Ciortea et al. 2010]	✓	×	×	×	✓	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	✓
[CSA 2014]	×	×	×	×	✓	✓	✓	×	×	×	×	×	×	×	×	×	×	×	×	✓	×	×	×
[De Capitani di Vimercati et al. 2013]	×	×	✓	×	×	×	✓	×	✓	×	×	×	✓	×	×	×	×	×	×	×	×	×	×
[De Capitani di Vimercati et al. 2014]	×	×	×	×	✓	✓	✓	✓	×	×	×	×	✓	×	×	✓	×	×	×	×	×	×	×
[Diallo et al. 2012]	×	✓	×	×	✓	×	×	×	×	×	×	✓	✓	×	×	×	×	×	×	×	×	×	×
[Doelitzscher et al. 2012]	×	×	×	×	✓	✓	×	✓	✓	✓	✓	✓	×	×	×	×	×	×	∼	✓	×	×	×
[Doelitzscher et al. 2013]	×	×	×	×	✓	✓	×	✓	✓	✓	✓	✓	×	×	×	×	×	×	∼	✓	×	×	×
[Doelitzscher et al. 2013]	×	×	×	×	✓	✓	×	✓	✓	✓	✓	✓	×	×	×	×	×	×	∼	✓	×	×	×
[Dsouza et al. 2013]	×	×	×	×	✓	×	×	✓	✓	✓	×	×	✓	×	×	×	×	×	×	×	×	×	×
[Ficco et al. 2013]	×	×	×	×	✓	✓	✓	✓	✓	✓	×	×	×	×	✓	×	×	×	×	×	×	×	×
[Foster and Spanoudakis 2011a]	✓	×	×	×	✓	✓	✓	×	×	×	×	×	×	×	×	×	×	×	✓	×	∼	×	×
[Foster and Spanoudakis 2011b]	×	✓	×	×	✓	✓	✓	×	×	×	×	×	×	×	×	×	×	×	✓	×	∼	×	×
[Gao et al. 2011]	×	×	✓	×	✓	✓	✓	✓	✓	✓	✓	✓	×	×	×	×	×	×	×	×	×	×	✓
[Garg et al. 2013]	×	✓	×	×	✓	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	✓	×	×
[Ghazizadeh et al. 2012]	×	×	×	✓	✓	×	×	×	×	×	✓	×	×	×	×	×	✓	×	×	×	×	×	×
[Godfrey and Zulkernine 2013]	×	✓	×	×	×	✓	×	✓	×	×	×	×	×	×	×	✓	×	×	×	×	×	×	×
[Grobauer et al. 2011]	×	✓	✓	×	✓	✓	✓	×	×	×	×	×	×	×	×	×	×	×	×	×	×	✓	×
[Hao et al. 2011]	×	×	✓	×	✓	✓	✓	×	✓	×	✓	✓	×	×	×	×	✓	×	×	×	×	×	×
[Hanawa et al. 2010]	×	✓	×	×	✓	✓	✓	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	✓
[Jajodia et al. 2013]	×	×	×	×	×	✓	✓	✓	×	✓	✓	✓	✓	×	×	×	×	×	×	×	×	×	×
[Jayasinghe et al. 2012]	×	✓	×	×	✓	✓	✓	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	✓
[Jhawar and Piuri 2013]	×	×	✓	×	×	✓	✓	×	×	✓	×	×	×	×	×	×	×	×	×	×	∼	×	×
[Jhawar et al. 2012]	×	×	×	✓	✓	✓	×	×	×	∼	×	∼	×	×	×	×	×	×	×	×	×	×	×
[Jin et al. 2013]	×	✓	×	×	×	✓	×	×	×	✓	×	×	×	×	×	×	×	×	×	×	✓	×	×
[Juels and Oprea 2013]	✓	×	×	×	×	✓	×	✓	✓	✓	×	×	✓	×	×	×	×	×	×	∼	×	×	×
[Jung et al. 2013]	×	✓	×	×	×	×	✓	×	×	×	×	✓	✓	×	×	✓	×	×	×	×	×	×	×
[Kai et al. 2013]	×	×	×	✓	✓	✓	✓	×	×	×	×	×	×	×	×	×	×	×	✓	×	×	×	×
[Kaaniche et al. 2013]	×	✓	×	×	✓	✓	✓	✓	×	×	×	✓	✓	×	×	×	×	×	×	×	×	×	×
[Khalid et al. 2013]	×	×	✓	×	✓	×	×	×	×	×	×	✓	×	×	×	×	✓	×	×	×	×	×	×
[Khan and Malluhi 2010]	×	×	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	×	×	×	∼	×	×	×	×	×	✓	×
[King and Ganti 2010]	×	✓	×	×	✓	✓	✓	✓	✓	✓	✓	×	×	×	×	×	×	×	×	×	×	×	✓
[Koeppe and Schneider 2010]	×	×	×	✓	×	✓	✓	×	×	×	×	×	×	×	×	×	×	×	✓	✓	✓	×	✓
[Krautheim 2009]	×	✓	×	×	✓	×	✓	✓	✓	×	×	✓	×	×	×	×	×	✓	×	×	×	×	×
[Krotsiani et al. 2013]	×	×	✓	×	✓	✓	✓	×	×	×	×	×	×	×	×	×	×	×	∼	×	×	✓	×
[Kurmus et al. 2011]	×	×	×	✓	×	✓	×	✓	✓	✓	×	×	×	×	×	✓	×	×	×	×	×	×	×
[Lang 2010]	×	×	×	✓	✓	×	×	✓	×	×	×	×	×	×	×	✓	×	×	∼	∼	×	×	×
[Lee et al. 2011]	✓	×	×	×	✓	✓	×	×	×	×	✓	×	×	×	✓	×	✓	×	✓	×	×	×	×
[Li et al. 2011a]	×	✓	×	×	×	✓	✓	✓	×	×	✓	×	✓	×	×	×	✓	×	×	×	×	×	×
[Li et al. 2011b]	×	✓	×	×	✓	✓	×	✓	✓	×	×	×	✓	×	✓	✓	×	×	×	×	×	×	×
[Li et al. 2013]	×	×	×	✓	×	✓	✓	×	×	×	×	✓	×	×	×	✓	×	×	∼	×	×	×	×
[Lin and Tzeng 2012]	×	✓	×	×	×	✓	✓	✓	×	✓	×	✓	✓	×	×	×	×	×	×	×	×	×	×
[Liu et al. 2013]	×	×	✓	×	✓	✓	✓	✓	×	×	✓	∼	×	×	×	✓	×	×	×	×	×	×	×
[Lombardi and Di Pietro 2010]	✓	×	×	×	×	✓	×	×	✓	×	×	×	×	×	×	✓	×	×	✓	×	×	×	×
[Lombardi and Di Pietro 2011]	×	×	✓	×	×	✓	×	×	✓	×	×	×	×	×	×	✓	×	×	✓	×	×	×	×
[Lu et al. 2014]	×	×	×	×	✓	✓	✓	×	×	✓	×	×	×	×	×	×	×	×	×	×	×	×	✓
[Luo et al. 2014]	×	×	×	×	✓	×	×	✓	✓	×	×	×	×	×	✓	×	×	×	×	×	×	×	×
[Ma et al. 2013]	×	×	×	✓	×	✓	✓	✓	×	✓	×	×	×	×	×	×	×	✓	×	×	×	×	×
[Mahmood et al. 2012]	×	✓	×	×	✓	✓	✓	✓	✓	✓	✓	×	×	×	×	×	×	×	×	×	×	×	✓
[Marinescu et al. 2013]	×	×	×	×	✓	✓	✓	×	×	×	×	×	×	×	×	×	×	×	×	×	×	∼	×
[Massie et al. 2012]	×	×	✓	×	✓	✓	✓	×	×	×	×	×	×	×	×	×	×	×	✓	×	×	×	×
[Mei et al. 2013]	×	×	✓	×	✓	×	✓	×	×	×	×	×	×	×	×	×	×	×	×	✓	×	×	×
[Meng and Liu 2013]	×	×	✓	×	✓	×	✓	×	×	×	×	×	×	×	×	×	×	×	✓	×	×	×	×
[Mohamaddiah et al. 2014]	✓	×	×	×	✓	✓	✓	×	×	×	×	×	×	×	×	×	×	×	✓	×	×	×	×

Table VI. Classification based on *when*, *where*, *what*, *how* dimensions (continued)

Reference (Year)	When				Where			What					How										
	1Q	2Q	3Q	4Q	AL	TT	PT	PC	PI	PA	PU	PP	E	S	I	AC	AU	TC	M	AD	SLA	C	T
[Modi et al. 2013b]	✓	×	×	×	✓	✓	×	✓	✓	✓	×	×	×	×	✓	×	×	×	×	×	×	×	×
[Monfared and Jaatun 2011]	×	×	×	✓	✓	✓	✓	✓	✓	✓	✓	✓	×	×	×	×	×	×	✓	×	×	×	×
[Moreno 2010]	×	×	✓	×	×	✓	×	×	×	✓	×	×	×	×	×	×	×	×	×	×	×	×	✓
[Mouratidis et al. 2013]	✓	×	×	×	×	×	✓	✓	✓	✓	✓	✓	×	×	×	×	×	×	×	×	✓	×	×
[Muñoz and Maña 2013]	×	✓	×	×	✓	✓	✓	✓	✓	✓	✓	✓	×	×	×	×	×	∼	×	×	×	✓	×
[Nabeel et al. 2013]	×	×	×	✓	✓	✓	×	✓	×	×	✓	×	✓	×	×	✓	×	×	×	×	×	×	×
[Nagios 2014]	×	×	×	×	✓	✓	✓	×	×	×	×	×	×	×	×	×	×	×	✓	×	×	×	×
[Ni et al. 2014]	×	×	×	×	×	✓	×	✓	✓	×	×	✓	✓	×	×	×	×	×	×	✓	×	×	×
[Okuhara et al. 2010]	×	×	×	✓	✓	×	×	✓	×	×	✓	×	×	×	×	✓	✓	×	×	×	×	×	×
[Pearson et al. 2009]	×	×	×	✓	✓	×	×	✓	×	×	×	✓	✓	×	×	∼	×	×	×	×	×	×	×
[Park et al. 2013]	×	×	✓	×	×	×	✓	×	✓	×	×	×	✓	×	×	×	×	∼	∼	×	∼	×	×
[Parveen and Tilley 2010]	×	✓	×	×	✓	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	✓
[Patel et al. 2013]	✓	×	×	×	✓	✓	×	✓	✓	✓	×	×	×	×	✓	×	×	×	×	×	×	×	×
[Pattuk et al. 2013]	×	✓	×	×	✓	×	∼	✓	×	×	×	✓	✓	×	×	×	×	×	×	×	×	×	×
[Peterson 2010]	×	×	✓	✓	✓	✓	×	✓	✓	×	✓	×	✓	×	×	✓	✓	×	×	∼	∼	×	×
[Pham et al. 2011]	×	✓	×	✓	✓	✓	✓	✓	✓	∼	×	×	×	×	×	×	×	×	×	×	×	×	✓
[Qin et al. 2013]	×	✓	×	×	✓	✓	✓	✓	×	×	✓	×	✓	✓	×	×	✓	×	×	×	×	×	×
[Rajkumar et al. 2013]	×	×	×	✓	×	✓	×	×	✓	✓	×	×	×	×	×	×	×	×	×	✓	×	×	×
[Rao et al. 2013]	✓	×	×	×	×	×	✓	×	×	×	×	×	×	×	×	×	×	×	✓	×	×	×	×
[Rasheed 2013]	×	×	×	✓	×	✓	✓	×	×	×	×	×	×	×	×	×	×	×	×	✓	×	×	×
[Raykova et al. 2012]	✓	×	×	×	×	×	✓	∼	×	×	×	✓	∼	×	×	✓	×	×	×	×	×	×	×
[Ruj et al. 2014]	✓	×	×	×	✓	×	×	×	×	×	✓	×	×	×	×	✓	×	×	×	×	×	×	×
[Sakr and Liu 2012]	×	✓	×	×	×	✓	×	×	×	×	×	×	×	×	×	×	×	×	×	×	✓	×	×
[Santos et al. 2012]	×	×	✓	×	✓	✓	✓	✓	✓	×	×	×	×	×	×	×	×	✓	×	×	×	×	×
[Sedayao et al. 2009]	×	×	×	✓	×	✓	✓	✓	×	×	×	×	✓	×	×	×	×	×	×	×	×	×	×
[Shao et al. 2010]	×	×	✓	×	✓	✓	✓	×	×	×	×	×	×	×	×	×	×	×	✓	×	×	×	×
[Shetty 2013]	×	✓	✓	×	×	✓	×	✓	✓	×	×	×	×	×	∼	×	×	×	∼	✓	×	×	×
[Shraer et al. 2010]	×	×	×	✓	×	×	✓	×	×	✓	×	×	×	✓	×	×	×	×	×	×	×	×	×
[Singhal et al. 2013]	✓	×	×	×	✓	✓	✓	✓	✓	×	×	✓	×	×	∼	✓	×	✓	×	×	×	×	×
[Song et al. 2009]	×	×	×	×	✓	×	×	✓	×	×	✓	×	×	×	×	×	✓	×	×	×	×	×	×
[Spanoudakis et al. 2012]	×	×	✓	×	✓	✓	✓	✓	✓	✓	✓	✓	×	×	×	×	×	×	×	×	×	✓	×
[Starov and Vilkomir 2013]	×	✓	×	×	✓	✓	✓	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	✓
[Stefanov et al. 2012]	×	×	×	✓	×	✓	✓	×	✓	✓	✓	×	×	×	×	×	✓	×	×	×	×	×	×
[Stolfo et al. 2012]	×	✓	×	×	✓	✓	×	✓	×	×	×	✓	×	×	✓	×	×	×	×	×	×	×	×
[Sulistio and Reich 2013]	×	×	✓	×	✓	×	×	✓	✓	✓	✓	✓	×	×	×	×	×	×	∼	×	✓	×	×
[Sundareswaran et al. 2012]	×	×	✓	×	×	×	✓	×	×	×	∼	×	×	×	×	×	×	×	✓	×	×	×	×
[Sunyaev and Schneider 2013]	✓	×	×	×	✓	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	✓	×
[Szefer and Lee 2014]	×	×	×	×	✓	✓	×	✓	✓	×	×	✓	×	×	×	×	×	✓	×	×	×	×	×
[Takabi and Joshi 2012]	✓	×	×	×	✓	×	×	✓	×	×	×	×	×	×	×	✓	×	×	×	×	×	×	×
[Takabi et al. 2010a]	×	×	✓	×	✓	✓	✓	✓	×	×	✓	✓	×	×	×	✓	✓	×	×	×	×	×	×
[Tang et al. 2012]	×	×	×	✓	✓	✓	×	✓	×	×	✓	×	✓	×	×	✓	×	×	×	×	×	×	×
[Thebeau II et al. 2014]	✓	×	×	×	✓	×	×	✓	✓	✓	×	×	✓	×	×	×	×	×	×	×	×	×	×
[Tysowski and Hasan 2013]	×	×	✓	×	×	×	✓	✓	×	×	×	✓	✓	×	×	×	×	×	×	×	×	×	×
[Tsai et al. 2011]	×	✓	✓	×	✓	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	✓
[van Dijk et al. 2012]	×	×	×	✓	×	×	✓	✓	×	×	×	×	✓	×	×	×	×	×	×	×	×	×	×
[Velten and Stumpf 2013]	×	×	×	✓	×	✓	✓	×	✓	×	×	×	×	×	×	×	×	✓	×	×	×	×	×
[Wan et al. 2012]	×	✓	×	×	✓	✓	×	✓	×	×	✓	×	✓	×	×	✓	×	×	×	×	×	×	×
[Wang et al. 2013]	×	✓	×	×	✓	✓	✓	×	✓	×	×	×	×	✓	×	×	×	×	×	✓	×	×	×
[Wang et al. 2010]	✓	×	×	×	✓	✓	✓	×	×	×	×	×	×	×	×	×	×	×	✓	✓	×	×	×
[Wang et al. 2010]	✓	×	×	×	×	×	✓	×	✓	×	×	∼	∼	×	×	×	×	×	×	✓	×	×	×
[Wang et al. 2011]	×	✓	×	×	×	✓	✓	×	✓	×	×	×	∼	∼	×	×	×	×	×	✓	×	×	×
[Wang et al. 2012]	×	×	✓	×	×	×	✓	×	×	×	×	✓	✓	×	×	×	×	×	×	×	×	×	×
[Wang et al. 2012]	×	✓	×	×	×	×	✓	×	✓	×	×	×	×	×	×	×	×	×	×	✓	×	×	×
[Wang et al. 2013b]	✓	×	×	×	×	×	✓	×	✓	×	×	∼	∼	×	×	×	×	×	×	✓	×	×	×
[Wang et al. 2014]	×	×	×	×	✓	×	✓	×	✓	×	×	✓	×	∼	×	×	×	×	×	✓	×	×	×
[Wang et al. 2013a]	×	×	✓	×	×	×	✓	×	✓	×	×	✓	×	✓	×	×	×	×	×	×	×	×	×
[Wei and Reiter 2013]	×	×	✓	×	✓	✓	✓	×	✓	×	✓	✓	✓	×	×	×	×	×	×	×	×	×	×
[Wei et al. 2013]	×	×	×	✓	✓	✓	×	×	✓	×	×	×	×	×	×	×	×	×	×	×	×	×	×
[Wei et al. 2014]	×	✓	×	×	✓	✓	×	×	×	×	✓	✓	×	×	×	×	×	×	×	✓	×	×	×
[Wei and Reiter 2012]	×	×	✓	×	✓	✓	✓	×	×	×	×	✓	✓	×	×	×	×	×	×	×	×	×	×
[Xing et al. 2013]	✓	×	×	×	✓	✓	✓	✓	✓	✓	✓	✓	×	×	✓	×	×	×	×	×	×	×	×
[Xu et al. 2013a]	×	×	×	✓	✓	×	×	×	×	×	✓	×	×	✓	×	×	✓	×	×	×	×	×	×
[Xu et al. 2013b]	×	✓	×	×	×	✓	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×
[Yang and Jia 2013]	×	×	✓	×	×	✓	×	✓	✓	×	×	✓	✓	×	×	×	×	×	×	✓	×	×	×
[Yang et al. 2013]	×	✓	×	×	✓	✓	×	✓	×	×	✓	×	✓	×	×	✓	×	×	×	×	×	×	×
[Ye et al. 2012]	×	×	×	✓	✓	✓	✓	×	×	×	×	×	×	×	×	×	×	×	×	×	×	✓	×
[Yu et al. 2013a]	×	×	✓	×	×	×	✓	×	×	×	×	✓	✓	×	×	×	×	×	×	×	×	×	×
[Yu et al. 2010a]	×	✓	×	×	✓	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	✓
[Yu et al. 2010b]	✓	×	×	×	×	✓	✓	✓	×	×	×	✓	✓	×	×	✓	×	×	×	×	×	×	×
[Yu et al. 2013b]	×	×	×	×	✓	×	×	×	×	✓	×	×	×	×	✓	×	×	×	×	×	×	×	×
[Zawoad et al. 2013]	×	✓	×	×	✓	✓	✓	✓	✓	×	×	✓	×	×	×	×	×	×	×	✓	×	×	×
[Zech 2011]	✓	×	×	×	✓	✓	✓	✓	✓	✓	✓	×	×	×	×	×	×	×	×	×	×	×	✓
[Zhang and Reiter 2013]	×	×	×	✓	×	✓	×	✓	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×
[Zhao et al. 2012]	✓	×	×	×	✓	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	✓	×	×
[Zhu et al. 2013]	×	✓	×	×	×	×	✓	×	✓	×	×	×	×	×	×	×	×	×	×	✓	×	×	×
[Zhu et al. 2012]	✓	×	×	×	✓	✓	×	✓	×	×	×	✓	✓	×	×	✓	×	×	×	×	×	×	×
[Zissis and Lekkas 2012]	✓	×	×	×	✓	×	×	✓	✓	×	✓	×	✓	×	×	×	×	×	×	×	×	×	×
[Zou et al. 2013]	×	×	×	✓	×	✓	✓	×	×	×	×	×	×	×	×	×	×	✓	✓	×	×	×	×

aspect is completely supported, ∼ means that it is supported but it is not the focus of the paper, × means that it is not supported.

C. COMPARISON WITH EXISTING SURVEYS AND WHITEPAPERS

After an initial period in which much cloud research and development have been devoted to the design, implementation, and refinement of basic cloud functionalities, in the last few years a lot of work has been done to secure the cloud and its users. Many

scientific articles have been published in international journals and conferences, and several surveys have tried to show an overall picture of the status of cloud security.

Fernandes et al. [Fernandes et al. 2013] provide a survey of cloud security solutions, which considers different key topics, including vulnerabilities, threats, and attacks, and proposes a taxonomy for their classification. The paper includes one of the most complete description of vulnerabilities, threats, and attacks to cloud infrastructures, characterizing them on the basis of their attack surface. The authors also report on the trend of cloud security publications between 2008-2012. Subashini and Kavitha [Subashini and Kavitha 2011] review security risks that could influence customer and provider activities in a cloud environment. They distinguish between security issues that affect IaaS, PaaS, and SaaS offerings. Considering IaaS level, the main problems for developers lie in the virtualization techniques and in the storage mechanisms used on physical hardware. At PaaS level, developers enjoy some degree of freedom for application management and deployment on top of the platform, while "under the hood" security issues are left in the provider's hands. In addition, security risks vary depending on the deployment model (private, public, and hybrid clouds) and are influenced by concerns similar to the ones faced by the traditional Internet infrastructure. Also at SaaS level clients must rely on security mechanisms implemented by the cloud provider. However, in SaaS scenario, it is even more difficult for users to evaluate the level of assurance and security guaranteed by the provider.[6] The authors claim that 14 key security elements must be considered at SaaS level: *i)* data security, *ii)* network security, *iii)* data locality, *iv)* data integrity, *v)* data segregation, *vi)* data access, *vii)* authentication and authorization, *viii)* data confidentiality, *ix)* web application security, *x)* data breaches, *xi)* virtualization vulnerability, *xii)* availability, *xiii)* backup, *xiv)* identity management and sign-on process. Hashizume et al. [Hashizume et al. 2013] analyze vulnerabilities, threats and attacks in the cloud, and outline possible countermeasures against them. At the end of 2012, Ryan [Ryan 2013] presented an overview of security in cloud computing focusing on open challenges. He identified four research directions in the context of confidentiality at SaaS level: fully homomorphic encryption, key translation in the browser, hardware-anchored security, and query processing over encrypted databases. Other work focuses on security at IaaS level [Dahbur et al. 2011; Dawoud et al. 2010]. Dahbur et al. [Dahbur et al. 2011] consider IaaS-level risks, threats, and vulnerabilities. Dawoud et al. [Dawoud et al. 2010] listed some typical security problems of IaaS implementation and deployment, and proposed some initial solutions. Vaquero et al. [Vaquero et al. 2011] discuss the impact of multi-tenancy on cloud security at IaaS level and remark that the majority of solutions include access control and encryption mechanisms, trying to guarantee well-known Confidentiality, Integrity, Availability (CIA) properties. Donevski et al. [Donevski et al. 2013] provide a security assessment methodology focusing on security threats posed by other tenants or other actors outside the cloud. The proposed methodology is tested on OpenStack [OpenStack Open Source Cloud Computing Software 2015], an open source IaaS solution for the cloud. Halton et al. [Halton and Rahman 2012] present a set of best practices for the integration and management of cloud security. Brender and Markov [Brender and Markov 2013] present a real study on risk perception and management in cloud computing, focusing on Swiss companies. Bouchenak et al. [Bouchenak et al. 2013] take a wider approach, and analyze existing tools for the verification of both functional and non-functional properties in the cloud, discussing challenges and new research directions.

In the line of the work discussed above, several whitepapers were published by stakeholder organizations. CSA released a set of security best practices for the

[6]We note that this problem paves the way to assurance solutions described in Section 5.

cloud [Cloud Security Alliance 2010; 2011]. In [Cloud Security Alliance 2010], CSA discusses guidelines for Identity and Access Management (IAM) in the cloud, which are fundamental for correct management of cloud services. In [Cloud Security Alliance 2011], a more general approach is taken, where cloud security guidelines are provided for critical areas focusing on 14 domains of interest. For each domain (e.g., governance and enterprise risk management, compliance and audit management, encryption and key management), a set of recommendations is provided. In turn, TrendMicro also published a whitepaper [Trend Micro 2013] discussing best practices for security and compliance with Amazon Web Services, while German Federal Office for Information Security (BSI) released a set of security recommendations for cloud computing providers [German Federal Office for Information Security 2012]. Similarly, the Cloud Standards Customer Council [Cloud Standards Customer Council 2012] listed the following 10 steps for achieving security in the cloud: *i)* ensure that effective governance, risk and compliance processes are in place, *ii)* audit operational and business processes, *iii)* manage people, roles, and identities, *iv)* ensure proper protection of data and information, *v)* enforce privacy policies, *vi)* assess security provisioning for cloud applications, *vii)* ensure that cloud networks and connections are secure, *viii)* evaluate security controls on physical infrastructures and facilities, *ix)* manage security terms in the cloud SLA, *x)* understand the security requirements of the exit process.

Some papers have surveyed together cloud security and privacy [Jansen and Grance 2011; Pearson 2013; Pearson and Benameur 2010; Takabi et al. 2010b; Xiao and Xiao 2013; Zhou et al. 2010]. Pearson et al. [Pearson et al. 2009] discuss how the concepts of privacy, security, and trust evolve with the advent of cloud, and outline possible approaches to their protection and management. Xiao and Xiao [Xiao and Xiao 2013] provide an extensive and complete overview of vulnerabilities, threats, and defenses in the context of cloud security and privacy. Similarly to our approach, this survey is organized according to security and privacy properties, and for each of them corresponding vulnerabilities, threats, and defenses are reviewed and analyzed. Zhou et al. [Zhou et al. 2010] first give an overview of security considering availability, confidentiality, data integrity, control, and audit in the cloud; then they show how existing approaches to privacy are doomed to fail in the cloud environment. Bohli et al. [Bohli et al. 2013] provide a survey of security and privacy solutions that build on the concept of simultaneous usage of multiple clouds. National Institute of Standards and Technology (NIST) [Jansen and Grance 2011] proposes a set of guidelines for achieving security and privacy in public cloud environments. Burger et al. [Burger et al. 2013] present a whitepaper from the TClouds project, whose aim is to provide the building blocks to implement a trustworthy cloud infrastructure. Other surveys focus on finer-grained aspects of cloud security like storage security [Aguiar et al. 2013; Paladi et al. 2013], virtualization security [Pearce et al. 2013; Perez-Botero et al. 2013], SaaS security in multi-tenant software platforms [Rodero-Merino et al. 2012], intrusion detection/prevention systems [Modi et al. 2013b]. Takahashi et al. [Takahashi et al. 2012] analyze the problem of guaranteeing security in a cloud multi-tenancy scenario. They explore the implication multi-tenancy could have on cloud security, and discuss the technical maturity of security approaches for multi-tenant cloud computing. In particular, they consider security issues at the following layers: hardware and software primitive layer, hypervisor layer, OS layer, application layer, and web security.

Iankoulova and Daneva [Iankoulova and Daneva 2012] point out that each cloud security solution focuses on a small subset of heterogeneous security requirements. Then, they focus on identifying general security requirements for cloud security and categorizing some of existing techniques based on them. In particular, they classify security requirements in 9 sub-areas: access control, attack/harm detection, non-repudiation, integrity, security auditing, physical protection, privacy, recovery, and

prosecution, where non-repudiation, physical protection, recovery, and prosecution count the smallest number of solutions, while access control, integrity, and auditability are the most researched sub-areas.

Our survey takes a different approach and studies the trend of cloud security assurance technique definition, with respect to the overall trend in cloud security solution definition, in the last few years (see Section 6.1).

D. STANDARDS AND PROJECTS

In this section, we complete our overview on the state of the art of cloud security and assurance by briefly reviewing existing cloud security standards, and research and development projects in the context of cloud security and assurance.

D.1. Standards

Many standards have been defined and are available for service-based ecosystems and distributed systems in general. Some of these standards might fit cloud requirements, while some others could require modifications to be applied in a cloud scenario. Some standards instead are completely missing and need to be designed from scratch to fit the cloud requirements.

In this context, the European Telecommunications Standards Institute (ETSI) [ETSI 2013] has led the effort done by the Cloud Standards Coordination (CSC) task force towards cloud standardization.[7] ETSI, a not-for-profit European Standards Organization recognized by the European Union that focuses on the specification of standards for ICT, has been in fact appointed by the European Commission to coordinate with stakeholders in the cloud standards ecosystems and devise standards roadmaps in support of EU policy in critical areas such as security, interoperability, data portability, and reversibility. The ETSI effort started at the end of 2012 and identified three main Technical Groups (TGs), namely, stakeholder roles and responsibilities (TG1), use cases selection/prioritization (TG2), and specification identification and gap analysis (TG3); TG3 was composed of three subgroups on: *i)* SLAs, *ii)* security and privacy, *iii)* interoperability, data portability, reversibility. The main goal of TG1 was the definition of all actors and parties involved in a cloud computing environment, having a role in the ETSI standardization process. Starting from the roles and responsibilities identified in TG1, the main goal of TG2 was the definition of a set of use cases and related requirements that can be of interest in a cloud computing environment. The main goal of TG3 was to analyze the use cases delivered by TG2, and identify existing standards and specifications that are relevant to cloud. In this context, TG3 surveyed these standards and identified existing gaps in their definition. The results of the work done by ETSI have been reported in [ETSI 2013]. After identifying use cases of interest for the cloud and their impact on standardization, the presented document maps the activities of the use cases on existing standards, specifications, reports, and whitepapers. Then, lessons learned, including a discussion of covered aspects and gaps, are provided. Finally, two annexes provide extensive and complete lists of standards, specifications, reports, and whitepapers that clearly present the status and landscape of cloud standards.

Following and completing the ETSI effort, a number of EU FP7 projects (ASSERT4SOA, Aniketos, Cirrus, CUMULUS, SPaCIoS, NeSSOS and SecCORD – see Appendix D.2) worked together to provide a gap analysis on cloud and service standardization in the context of assurance and certification techniques. The document, which has been presented to ETSI, is available at [Aniketos, ASSERT4SOA, CUMULUS, SecCord 2013].

[7] http://csc.etsi.org/website/home.aspx

Finally, it is important to mention the ISO/IEC 27018 "Code of practice for data protection controls for public cloud computing services" standard that will provide guidance on the privacy elements/aspects of public clouds. It is accompanied by ISO/IEC 27017 covering the wider information security angles. ISO/IEC 27018 is not intended to duplicate or modify ISO/IEC 27002 in relation to cloud computing, but it will add control objectives and controls relevant to the protection of privacy and personal data in the cloud.

D.2. Projects

In the last years, several organizations and research projects have focused on increasing the security of distributed systems in general and cloud computing in particular. Among them, NIST [Jansen and Grance 2011; Mell and Grance 2011] first focused on the definition of main cloud concepts, roles, and fundamentals, and then distributed a set of recommendations (NIST SP-800-144) on security and privacy in the cloud. Following a similar approach, ENISA focused on security assurance and risk evaluation in the cloud [Catteddu and Hogben 2009a; 2009b] and on security SLAs and security monitoring [Dekker and Hogben 2011; Hogben and Dekker 2012]. As already mentioned in this survey, CSA has been very active in analyzing security, privacy, and trust issues in the cloud [Cloud Security Alliance 2010; 2011]. Finally, the Federal Risk and Authorization Management Program (FedRAMP) provided a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. In particular, it released a document describing best practices for acquiring IT as a service [CIO 2012].

In addition to the above efforts, several EU FP7 research projects focused on increasing security of distributed systems. Early projects focused on securing SOA and their applications. ASSERT4SOA [Advanced Security Service cERTificate for SOA 2010] was aimed at supporting new certification scenarios, where the security certification of services is required and plays a major role. ASSERT4SOA has produced novel techniques, tools, and an architecture for expressing, assessing, and certifying security properties for complex service-oriented applications, composed of distributed software services that may dynamically be selected, assembled and replaced, and running within complex and continuously evolving software ecosystems. SLA@SOI [Empowering the service industry with SLA-aware infrastructures 2008] focused on the design and implementation of an architecture and different approaches for the management of SLAs in service-oriented and cloud infrastructures. It also defined a language called SLA-* supporting the description of generic SLAs and provided a suite of open source software supporting the implementation of SLA-aware services. PoSecCo [Policy and Security Configuration Management 2010] analyzed the problem of security compliance and automatic security configuration of services. In particular, it focuses on refining high-level security requirements in abstract low-level security configurations, using a product-independent syntax and format. Low-level configurations are then mapped and translated to fit the actual system syntax, format, and requirements. PoSecCo also provided solutions for the maintenance of such configurations in the final product. ANIKETOS [Ensuring Trustworthiness and Security in Service Composition 2010] considered the problem of ensuring security and trustworthiness of services, which are composed dynamically at runtime. It provided methods to analyze new threats and vulnerabilities, and solve them by providing a platform for security and trust management of composite services. SPaCIoS [Secure Provision and Consumption in the Internet of Services 2010] focused on the validation and verification of services both at static (before service provisioning) and production (after service deployment) time. The project aimed to provide new techniques for service validation and verification based on penetration testing, security testing, model checking, and

automatic learning. In turn, Nessos [Network of Excellence on Engineering Secure Future Internet Software Services and Systems 2010] has analyzed the problem of engineering secure software-based services and systems. The project vision is based on the idea that this kind of goal can be only achieved by addressing security concerns from the beginning of system analysis and design. This approach can in fact reduce the probability of service vulnerabilities and integrate security treatment within the engineering process.

More recently, other EU FP7 research projects focused on defining solutions and infrastructures to secure the cloud. CloudSec [CloudSec 2013] is a joint research project between Telenor and SINTEF, which has prepared a checklist for cloud security. The project allows customers to identify their requirements on cloud providers and compare them on the basis of a systematic approach. CIRRUS [Certification, InteRnationalisation and standaRdization in cloUd Security 2012] focuses on solutions for security and privacy in cloud computing. It aims to address those security and privacy concerns introduced by the need of moving sensitive services and data to the cloud, migrating data between different cloud providers, and facilitating businesses in joining the cloud infrastructure. CIRRUS launched the CEN/CENELEC workshop on Requirements and Recommendations for Assurance in the Cloud (CEN-WS RACS) [CEN 2014] aimed to provide recommendations for future cloud assurance standards. A4Cloud [Cloud Accountability Project 2012] deals with audit and accountability in the cloud. It is aimed at increasing trust in the cloud, by producing approaches and tools that allow cloud providers to be accountable for the privacy and confidentiality of information. These approaches and tools include risk analysis, policy enforcement, monitoring, and compliance auditing. SPECS [Secure Provisioning of Cloud Services based on SLA management 2013] focuses on the realization of a framework supporting techniques and tools for user-centric negotiation of security parameters in SLA, monitoring-based verification of SLAs, and enforcement of SLAs in the cloud. CUMULUS [Certification infrastrUcture for MUlti-layer cloUd Services 2013] comes as an extension to the work done in ASSERT4SOA and aims to provide a new security certification scheme for the cloud. CUMULUS is focusing on developing an integrated framework of models, processes, and tools supporting the certification of security properties at infrastructure (IaaS), platform (PaaS), and software application (SaaS) layers. Its final goal is to put service users, service providers, and cloud suppliers together with certification authorities to ensure security certificate validity in the cloud. Broker@Cloud [Continuous Quality Assurance and Optimisation for Cloud brokers 2012] focuses on providing an enhanced brokerage framework allowing cloud intermediaries to support continuous quality assurance and optimization of service-based software in the cloud. Finally, RESERVOIR [Resources and Services Virtualization without Barriers 2008] demonstrates how virtual machines could be migrated between different hosts, enables smaller infrastructure providers to collaborate through the federation of their resources on demand, and provides first approaches to cloud elasticity.

Finally, also research projects funded by the US National Science Foundation (NSF) focused on different aspects of cloud security and assurance. To name but a few, Secure Data-Intensive Computing on Hybrid Clouds project [Secure Data-Intensive Computing on Hybrid Clouds 2012] considers the problems of *i)* protecting privacy of data intensive computations in the cloud and *ii)* increasing privacy assurance on data management practices. Secure and Privacy-assured Data Service Outsourcing in Cloud Computing project [Secure and Privacy-assured Data Service Outsourcing in Cloud Computing 2012] aims to provide a security- and privacy-enhanced outsourcing solution for the cloud based on an encrypted cloud data service, a cloud data sharing service, and a privacy-preserving secure cloud storage auditing. Infrastructure for Secure Cloud Computing project [Infrastructure for Secure Cloud Computing 2013] focuses

on securing two important aspects of the cloud: resource sharing and fine-grained pricing. Risk Assessment Techniques for Off-line and On-line Security Evaluation of Cloud Computing project [Risk Assessment Techniques for Off-line and On-line Security Evaluation of Cloud Computing 2013] considers the need of a security risk evaluation framework for cloud computing. It focuses on off-line risk management and on-line trust evaluation, and aims to support users in the evaluation of cloud service/resource trustworthiness. Cloud Security on Demand project [Cloud Security on Demand 2012] proposes a solution to on-demand security, where security requirements and policies are automatically mapped on appropriate cloud deployments and their support continuously verified at runtime.