Olga Wenge, Melanie Siebenhaar, Ulrich Lampe, Dieter Schuller, Ralf Steinmetz:
Much Ado about Security Appeal: Cloud Provider Collaborations and Their Risks.
In: Proceedings of the 1st European Conference on Service-Oriented and Cloud Computing (ESOCC 2012), Springer, September 2012.

Much Ado about Security Appeal: Cloud Provider Collaborations and their Risks

Olga Wenge, Melanie Siebenhaar, Ulrich Lampe, Dieter Schuller, Ralf Steinmetz

Multimedia Communication Lab (KOM)
Technische Universität Darmstadt, Germany
e-mail: {firstname.lastname}@KOM.tu-darmstadt.de

Abstract. The lack of capacity, unplanned outages of sub-contractors, a disaster recovery plan or financial goals may force cloud providers to enter into collaborations with other cloud providers. However, the cloud provider is not always fully aware of the security level of a potential collaborative cloud provider. This can lead to security breaches and customers' data leakage, ending in court cases and financial penalties. In our paper, we analyze different types of cloud collaborations with respect to their security concerns and discuss possible solutions. We also outline trusted security entities as feasible approach for managing security governance risks and propose our security broker solution for ad hoc cloud collaborations. Our work provides support in the cloud provider selection process and can be used by cloud providers as a foundation for their initial risk assessment.

Keywords: cloud computing security, cloud collaborations, data privacy, data protection, security broker

1 Introduction

Nowadays, cloud computing is widely spread in very different industries due to its efficiency, scalability and cost-saving models. The collaboration of clouds opens new perspectives for cloud providers, helping to mitigate technical risks, assure availability and provide customers with a large range of services. Sometimes, cloud providers *are forced* to enter collaboration immediately, because of an unplanned disaster, as a backup solution, or because of some political and economical decisions.

However, the selection process of a potential collaborative cloud is not trivial. An "ideal" collaborative cloud must fully meet all requirements and criteria, a cloud provider identified for the collaboration. The requirements may include technical aspects, pricing, unique cloud services, mutual benefits, and last but not least – a big bouquet of security requirements.

Security requirements may vary between cloud providers, depending on their business needs, security policies and data classification. In our paper, we define and discuss

possible types of cloud collaborations and their security issues, as well as their possible solutions.

The paper is structured as follows: In Section 2, we discuss different types of multiple clouds and give a holistic definition of cloud collaborations with respect to security metrics. Section 3 provides an overview and evaluation of security risks in cloud collaborations and their possible solutions. In Section 4, we outline security governance issues in cloud collaborations and discuss trusted security entities (TSEs). We propose here our security broker selection process as a solution for ad hoc collaborations. Finally, Section 5 describes our future work.

2 Security aware cloud collaboration types

In recent papers about cloud computing many different definitions can be found related to cloud collaborations. Keahey et al. [1] define dynamically provisioned distributed domains over several clouds as *"sky computing"*; Bernstein and Vjj [2] describe *"intercloud"* as *"a network of clouds"* and Wolf et al. [3] as *"Cloud of clouds"*, while Kretzschmar et al. [4] use the *"multi-cloud"* term for their definition; *federation of clouds* is defined by Wolf et al. [3] as "a homogenous environment, where all partners use the same standard". Almutairi et al. [5] propose another view of cloud collaborations with respect to security access control: *federated collaborations* with a metapolicy for the cloud access control, loosely *coupled collaborations* with local security policies for the access control, and *ad hoc collaboration* with the third party provider as a trusted partner for access control verification. The authors measure tradeoffs between proposed types of collaboration using the following four metrics: *level of interoperation* between cloud providers, their *autonomy*, *level of privacy*, and *verification complexity* of security policies.

In our paper we present a holistic security analysis and explore these three types of cloud collaborations as proposed by Almutairi et al. [5] with respect to further security risk metrics, which Cloud Security Alliance (CSA) considers as the critical areas of cloud computing [6]:

- Legal risk
- Proprietary definitions of cloud services and deployment models
- Compliance and audit with regulators
- Insufficient level of security
- Data protection risk
- Data location risk
- Identity and data access risks
- Monitoring and incident response issues
- Interoperability and portability risk
- Cloud governance risk

We extend the proposed by Almutairi et al. [5] definitions of the cloud collaborations with respect to the classical security domains [7], and define the cloud collaboration types as follows:

Federated collaborations presume a global *metapolicy*, which is conform and compliant with all policies of all collaborative partners. Policies can include security policies, data privacy policies, data classification policies, regulators requirements, and local laws. Compliance of all collaborative partners leads to a strong mutual dependence and trusted interoperation between individual clouds, i.e. all clouds within a federation can interoperate without *"security fear"*.

A loosely coupled collaboration allows more autonomy and is managed by local policies between collaborative partners, e.g. service level agreements (SLAs) or other preagreed collaboration contracts, which fully meet security requirements of both cloud providers.

An ad hoc collaboration does not set any predetermined agreement or rules between individual clouds. The selection of a collaboration partner performs in a dynamic "ad hoc" manner and can be denied if an individual cloud did not persuade with his "security appeal", e.g. sufficient authentication and authorization mechanisms, network encryption, etc. By ad hoc collaboration, cloud providers need some kind of trustable security interface for security judgment: a trusted security entity (TSE).

Fig.1 gives a graphical overview of the cloud collaboration types as described before and tradeoffs between them.

3 Security concerns and solutions in multiple cloud environments

In this section, we outline security concerns and issues of the defined types of cloud collaboration with respect to the critical areas, proposed in Section 2.

3.1 Legal risks

The lack of international standards for data privacy and data transfer is one of the major hurdles for cloud providers. The recent legislations in EU (European Data Protection Directive – Directive 9/46/EC) [8] and Canada (Canada's Personal Information Protection and Electronic Document Act – PIPEDA) [9] restrict transfer of customers' personal data to countries without *"an adequate level of protection"* [10].

While Europe and Canada believe *society* is responsible for protection of private data, the USA considers *individual users* to be responsible for protecting their own data [11]. In some countries data protection laws are still not implemented, as for example in Malaysia [12], or only partly implemented, as in Taiwan [13].

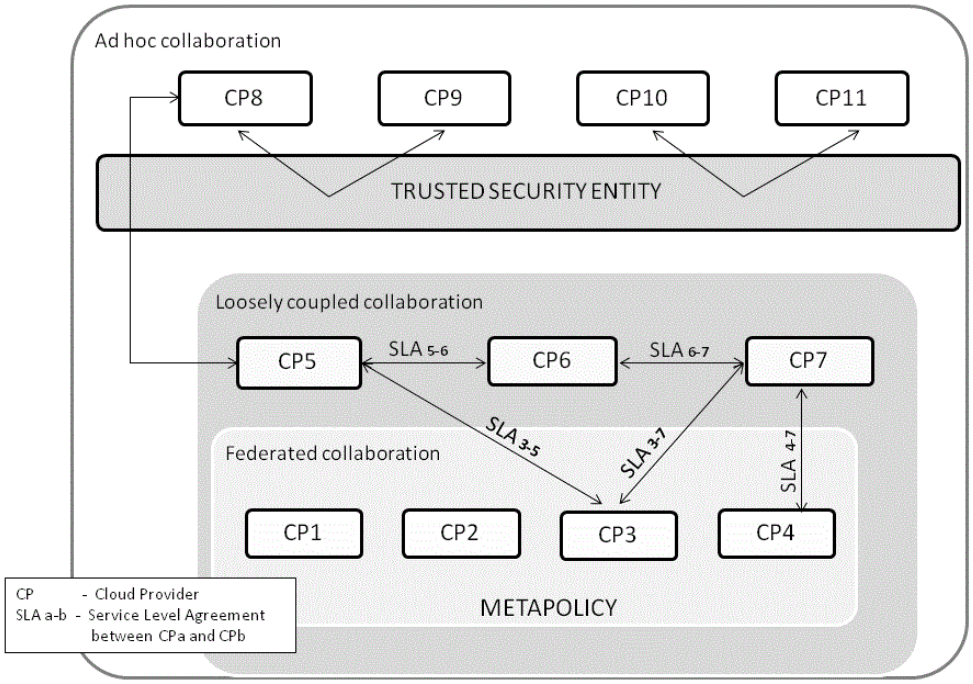

Fig. 1. Cloud collaboration types and their tradeoffs.

Poor knowledge of laws can lead to privacy breaches; therefore, all cloud providers should be aware of countries' actual laws about data privacy, data protection and other laws, related to their services and collaborative partners.

European Network an Information Agency (ENISA) [14] recommends *a fully awareness* of laws and government regulations to be prepared contractually to cooperate with cloud providers from different legal environments. Cloud providers can also implement their own *additional privacy policies* to provide the necessary level of trust [15]. Additional policies must include directives concerning collecting, recording, using, or storing of data and agreed upon with customers, because in some countries, cloud providers cannot transfer data to another provider without customers' explicit permission [11].

Adoption of international policies, such as Organization for Economic Co-operation and Development (OECD) or Asia-Pacific Economic Cooperation (APEC) guidelines [14] could be a feasible solution as well, especially for ad hoc collaborations [15]. An agreement on global privacy laws could be *a panacea* against international cyber security issues, but this approach is very challenging and complex, because of heterogeneities of local laws and political situations [16].

So, the weaker the collaboration bindings, the higher the risks. We depict our observed dependencies between the cloud collaboration types and security risk in the Fig 2.

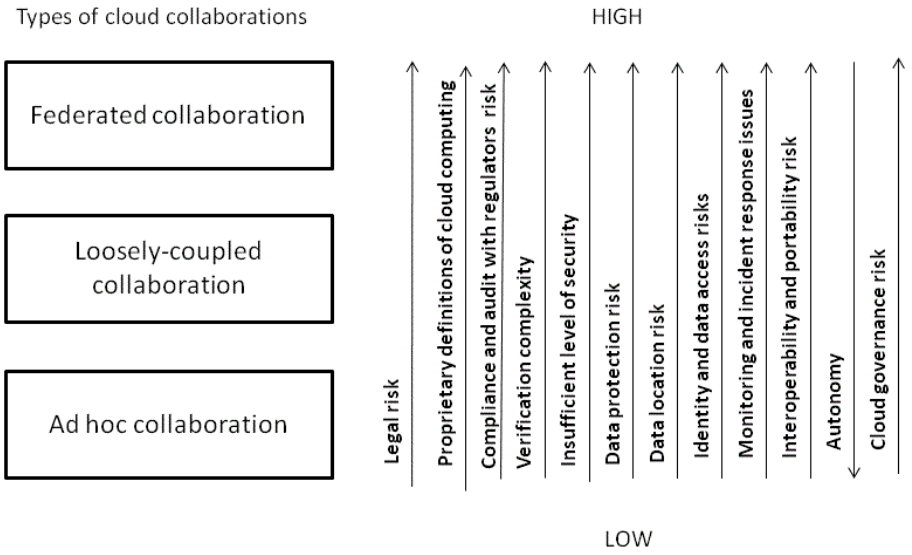

Fig. 2. Evaluation of proposed security metrics in cloud collaborations.

3.2 Proprietary definitions of cloud services and deployment models

The variety of different non-standardized definitions of cloud computing, cloud service models (Infrastructure-as-a-Service, Platform-as-a-Service, Software-as-a-Service, Database-as-a-Service, Business-as-a-Service, etc.), and cloud deployment models (private, public, community, hybrid, virtual-private hybrid, etc.) could be another issue for proper collaboration between cloud providers, especially in ad hoc manner. The differences on definitions can cause security discrepancy and make the cloud provider vulnerable, e.g. if a database with related security configurations is defined as a part of Platform-as-a-Service by one cloud provider and not by another one.

To avoid these misunderstandings and possible trials with customers, only pre-agreed definitions must be used in the collaboration (e.g. according to National Institute of Standards and Technology (NIST) definitions, cloud reference model [17], cloud taxonomy definition [6]) and documented in SLAs [18].

3.3 Compliance and Audit with regulators

Compliance resolutions with regulators for special industries, such as banking, health care, government, must be taken into consideration by selecting a potential collaboration partner. Different industries must be compliant with special industrial standards and laws, e.g. financial institutions operating in the USA must be compliant to Sarbanes-Oxley (Sox) Act [11], and in Europe – with Basel II [14]; medical institutions in the USA must be compliant with Health Insurance Portability and Accountability Act - HIPAA [15].

Therefore, cloud provider must be aware of these requirements and be ready to reflect them in their contracts or contracts with third-party auditors. The complexity of the verification of special regulations and their adoption in contacts is very high and time-consuming, therefore not applicable for dynamic ad hoc collaboration with individual clouds without required compliance evidence.

In addition, proper security monitoring agreements should be established for sufficient evidence of secure collaboration. Some effective common certification assurance frameworks and risk assessments for (cloud) providers, such as ISO/IEC 27001/27017 [19], COBIT [20], Cloud Security Alliance Control Matrix [21], Bundesamt für Sicherheit in der Informationstechnik (BSI, in Germany) Recommendation for Cloud Providers [22], and Shared Assessment Program [23], can be used as a basis for security control agreements for federative and loosely coupled collaborations, and as a compliance evidence for individual clouds in the ad hoc collaboration.

3.4 Insufficient level of security

Before transferring the customers' data to a collaboration partner, the cloud provider must be aware of the security level of a collaborative partner to prevent the compromising of data protection and data privacy laws.

The security assurance of a potential collaborative cloud provider can be provided via a trusted cloud provider certification, risk assessment or information security policy with defined security controls, necessary for a planned type of collaboration [6].

Actual security policies and risk assessments should include all relevant security domains, recommended by security standard institutions such as NIST [24], ISO/IEC 27001/27017 [19], BSI [23] and Information Systems Audit and Control Association (ISACA) [25]:

- Access control
- Encryption and key management
- Security governance
- Network security
- Business continuity management and disaster recovery,

- Security monitoring
- Application and infrastructure security
- Physical security
- Virtualization security

The review of policies and assessment results of collaborative partners should be taken to identify their security level and to make a decision on a possible interoperation. The security level of a potential collaborative partner should be at least equal to the cloud provider's level [22].

In the ad hoc collaboration a trusted security entity (e.g., a security broker, a trusted third party) is necessary for a proper decision.

3.5 Data protection issues

The data transferring to a collaborative partner should be protected at least at the same level as by the origin cloud provider [22]. Differences between proprietary data protection mechanisms can lead to security gaps and data compromising.

Agreed data classification or data labeling framework is one of the solutions to identify the needed protection level for data flow. Watson [12] proposes an extended Bell-LaPadula security model for cloud providers, where decision of data transfer in the multi-level security environment depends on the sensitivity of the data. Role-based access control (RBAC) models for cloud, defined by Berger et al. [13] can be used for automated identification of the data protection level and for assigning a level to a potential collaborative partner for interoperations.

To prevent data leakage and provide data integrity, collaborative cloud providers should use pre-agreed data content patterns, encryption mechanisms and best practice key management solutions, such as trusted platform modules (TPMs), one-time passwords [28], etc.

An implemented data retention policy is also a "nice-to-have" solution for data misuse after service delivery.

3.6 Data location risk

A cloud provider must be aware of data location if he transfers the users' data to another cloud provider to be compliant with customers' SLAs and other specific regulations described in Section 3.1 and Section 3.3. Proper defined SLAs with collaborative partners are one of the solutions to prevent non-controlled data movements [29].

3.7 Identity and Data Access risks

Identity and data access in multiple cloud environments is one of the most serious issues because of its complexity and involvement of several classical security domains: encryption, key management, information security, application and infrastructure security. The idea of the *cross-cloud identity and data access* is a dynamic, quick and customer friendly cloud service. The issues of non-proper and non-secure identity and access management are non-standardized identification, authentication and authorization mechanisms between cloud providers.

A *centralized* identity and access administration and governance has to be replaced with a *decentralized* one, because of the overwhelming number of rules to be managed [5]. Secure federated cloud access mechanisms and *good access practices*, such as Security Assertion Markup Language (SAML), secure single-sign-on [30], as possible solutions should be implemented between cloud providers. Sabahi [31] proposes a control access to all levels, including virtual machines (VMs), and Almutairi et al. [5] bet on a *fine-grained authorization mechanism*, multi-factor authentication and distributed access control architecture. Wolf et al. [3] propose a "message meta model for federated authentication for heterogeneous clouds across different standards", which can be used for ad hoc collaboration as well.

3.8 Insufficient monitoring and incident response

Security monitoring and security incident management are eminent parts of a proper security concept for every cloud provider. An efficiently implemented security monitoring, using a combination of preventive, detective and corrective measurements, can save lots of money, reputation and troubles, if a cloud provider knows what should be monitored. Many researchers are busy with the mapping of traditional security monitoring frameworks to a cloud computing architecture, to define gaps and provide new monitoring metrics. ENISA in "A guide to monitoring of security service levels in cloud contracts" [32] proposes different monitoring parameters for Infrastructure-as-a-Service, Platform-as-a-Service and Software-as-a-Service, including requirements for log management, incidence response, and forensics.

It is strongly recommended to define all *monitoring parameters* and related *vulnerability and incident response processes* in the SLAs with a collaborative partner or with a third-party monitoring provider. Sufficient monitoring evidences can be used to identify fraud, zero-day attacks and support IT forensic science.

3.9 Portability, Interoperability and Autonomy

Almost all cloud providers use their own proprietary security solutions for their services, and do not make them public because of intellectual property rights, hacking issues and other business concerns. The lack of public information ends up with a provider *lock-in* and hampers customer's portability and interoperability.

ENISA [14] and CSA [6] recommend using only standard technologies and solutions for collabo-ration to avoid a cloud provider lock-in, or to sign a so-called *escrow agreement* in case a cloud provider stops its activity.

As we already mentioned above, federated collaborations assume a high level of *mutual interoperability* and low level of *autonomy*, in comparison to ad hoc collaboration. But, if any security threat occurs in the federation, it will compromise all collaborative partners, as they use one metapolicy.

Viability and capability of a cloud provider is another very important aspect. A potential collaborative partner should provide the existence of *Plan B* – a business continuity and disaster recovery plan, which is especially critical for interoperability with high available and sensitive data [31].

We present our evaluation of described risks in Fig.2; the arrow head shows the highest value.

4 Security governance in the cloud collaborations

In this section, we discuss a *trusted security entity (TSE)* as possible solution for security governance risks and propose our initial TSE approach, which we plan to develop in our future work.

Security governance in the federated or loosely coupled collaborations is regulated by metapolicy, SLAs or a contracted security provider. The lack of a standardized trusted security entity (TSE) makes the ad hoc collaboration between clouds very difficult. Requests for the necessary security evidence of a potential collaborative partner and responses to it cannot be provided dynamically and without latency. A cloud provider must be *fully aware* of his own security requirements (security policy, SLAs, security standards, etc) to determine security requirements and map them against the TSE output.

To the best of our knowledge there are very different approaches of a TSE for federated or loosely coupled cloud collaborations. Huang et al. [33] propose an *"identity federation broker"*, based on an interaction of transitive federated single sign-on principle. Goyal [34] defines a distributed security method to "end-2-end services security for heterogeneous cloud environments". His method does not require a centralized infrastructure and based on *the mutual methods of trust and security* used for public key infrastructure (PKI). Ates et al. [35] bet on *"an identity cloud agent"* and propose an *Identity-as-a-Service* approach.

The Shared Assessment Program [23] is an industrial standard self-assessment for cloud providers and third party auditors, and can be used as a standard in the federated collaboration.

CSA [6] recommends the following *five-steps methodology* to identify a potential cloud-ready asset and a potential cloud partner: "1) Identify the asset; 2) Evaluate the asset; 3) Map the asset to the potential cloud deployment model; 4) Evaluate potential cloud service models and providers; and 5) Map out the potential data flow " .

However, the proposed TSE approaches are generally *hardly* applicable to ad hoc cloud collaborations. We suggest the following *six-step TSE selection approach*, our *security broker*, which we consider to be applicable for ad hoc collaborations as well:

Step 1: Security broker performs or gathers security risk assessments of each potential cloud provider, eager to collaborate;

Step 2: Security broker classifies risk assessments results and store these results in his database;

Step 3: A cloud provider X sends a specified collaboration request, which include cloud provider's security requirements and description of the expected security level of a potential collaborative cloud;

Step 4: Security broker analyzes and classifies requirements of a cloud provider X;

Step 5: Security broker maps the classified results with the results of security risk as-assessments in his data base to identify an appropriate collaborative cloud provider;

Step 6: Security broker outputs nothing or a list with recommended cloud providers.

Our proposed security broker approach can be used in all types of cloud collaboration, described in Section 2. While Storing and classifying of performed security risk assessments of cloud providers, the verification complexity can be avoided, that makes our security broker also applicable for ad hoc collaborations. To provide a proper selection process, our proposed approach needs to be completed with *a proper security assessment classification* and with defined *mapping rules*, which we aim to provide in the future.

5 Conclusion and future work

In our paper, we defined different types of cloud collaborations with respect to their security issues and discussed potential solutions. We could see that the different types of cloud collaborations either tend increase or decrease described cloud security risks.

Hence, the determination of the risk level indicates whether a specific collaboration type is appropriate or not to conduct the risk assessment.

We have also proposed the application of a *trusted security entity (TSE)* – our *security broker* - for ad hoc collaborations and a corresponding cloud provider selection process.

In the future, we plan to analyze cloud providers' collaboration requirements in more details in order to define a holistic security framework for an "ideal" *cloud security broker*, we outlined in Section 4.

REFERENCES

1. Keahey et al., "Sky Computing", IEEE Internet Computing, September/October 2009, pp. 43-51.
2. Bernstein et al., "Intercloud Security Considerations", Proceedings of IEEE International Conference on Cloud Computing Technology and Services, 2010, pp. 537-544.
3. Wolf et al., "A Message Meta Model for Federated Authentication in Service-oriented Architectures", IEEE International Conference on Service-Oriented Computing and Applications (SOCA), 2009 , pp. 1-8
4. Kretzschmar et al., "Security management Spectrum in future Multi-Provider Inter-Cloud Environments – Method to highlight necessary further development", 5th International DMTF Academic Alliance Workshop on Systems and Virtualization Management (SVM), 2011, pp. 1-8.
5. Almutairi et al., "A Distributed Access control Architecture for Cloud Computing", Software, IEEE Volume: 29, Issue: 2, 2012, pp. 36 – 44.
6. CSA, "Security Guidance for Critical Areas of Focus in Cloud Computing", V3.0, https://cloudsecurityalliance.org/research/security-guidance/
7. "CISSP Domains", https://www.isc2.org/cissp-domains/default.aspx
8. European Data Protection Directive – Directive 9/46/EC, http://eurex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:0050:EN:PDF
9. Canada's Personal Information Protection and Electronic Document Act – PIPEDA, http://www.priv.gc.ca/leg_c/leg_c_p_e.asp
10. Pearson et al., "Privacy, Security and Trust Issues Arising from Cloud Comp-ting", IEEE Second International Conference on Cloud Computing Technology and Science (CloudCom), 2010, pp.: 693 – 702.
11. Perkins et al., "Multinational Data-Privacy Laws: An Introduction for IT Managers", Professional Communication, IEEE Transactions on Volume: 47 , Issue: 2, 2004, pp. 85 – 94.
12. Ho et al., "A Guideline to Enforce Data Protection and Privacy Digital Laws in Malaysia", Second International Conference on Computer Research and Development, 2010, pp. 3 – 6.
13. Chen et al., "Legal Issues on Public Access to Remote Sensing Data in Taiwan", Geosciences and Remote Sensing Symposium, 2005.
14. ENISA, "Security & Resilience in Governmental Clouds", 2011, http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds

15. Wood et al., “Understanding the complexity surrounding multitenancy in cloud computing”, IEEE 8th International Conference on e-Business Engineering (ICEBE), 2011, pp. 119 – 124.
16. Wolf, C., “The Role of Government in Commercial Cybersecurity”, Telecom World (ITU WT), Technical Symposium at ITU, 2011, pp. 13 – 18.
17. NIST SP 800-145, The NIST Definition of Cloud Computing, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
18. Brensmed et al., “Security SLAs for Federated Cloud Services”, Sixth International Conference on Availability, Reliability and Security (ARES), 2011, pp. 202 – 209.
19. ISO/IEC 27001, International Standard, 2005, http://www.iso.org/iso/catalogue_detail?csnumber=42103
20. COBIT, http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx
21. CSA Cloud Control Matrix, https://cloudsecurityalliance.org/research/ccm/
22. BSI-Standard 100-1, Version1.5, https://www.bsi.bund.de/ContentBSI/Publikationen/BSI_Standard/it_grundschutzstandards.html
23. The Shared Assessment Program, „Evaluation Cloud Risk for the Enterprise: A Shared Assessment Guide“, 2010, http://sharedassessments.org/media/pdf-EnterpriseCloud-SA.pdf
24. NIST, “Guide for Security-Focused Configuration management of Information Systems”, 2011, http://csrc.nist.gov/publications/nistpubs/800-128/sp800-128.pdf
25. ISACA, “Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives”, 2011.
26. Watson, P., “A Multi-level Security Model for Partitioning Workflows over federated Clouds”, IEEE Third International Conference on Cloud Computing Technology and Science (CloudCom), 2011, pp. 180 – 188.
27. Berger et al., “Security for the Cloud Infrastructure: Trusted Virtual Data Center Implementation”, IBM Journal of Research and Development, Volume: 53, Issue: 4, 2009, pp. 6:1 - 6:12.
28. Wu et al., “Alignment of Authentication Information for Trusted Federation”, EDOC Conference Workshop, 2007, pp. 73 – 80.
29. Kandukuri et al., “Cloud Security Issues”, Services Computing, 2009, pp. 517 – 520.
30. OASIS-Security-Services, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security
31. Sabahi, F., “Cloud Computing Security Threats and Responses”, IEEE 3rd International Conference on Communication Software and Networks, 2011, pp. 245 – 249.
32. ENISA, “Procure Secure: A guide to monitoring of security service levels”, 2012, http://www.enisa.europa.eu/activities/application-security/test/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts
33. Huang et al., “Identity Federation Broker for Service Cloud”, International Conference on Service Sciences (ICSS), 2010, pp. 115 – 120.
34. Goyal, P., “Application of a Distributed Security Method to End-2-End Services Security in Independent Heterogeneous Cloud Computing Environments”, IEEE World Congress on Services (SERVICES), 2011, pp. 379 – 384.
35. Ates et al., “An Identity-Centric Internet: Identity in the Cloud, Identity as a Service and other delights”, Sixth International Conference on Availability, Reliability and Security (ARES), 2011, pp. 555 – 560.