Olga Wenge, Dieter Schuller and Ralf Steinmetz:
Towards Establishing Security-Aware Cloud Markets. In: Proceedings of the 6th International Conference on Cloud Computing (CloudCom), December 2014.

Towards Establishing Security-Aware Cloud Markets

Olga Wenge, Dieter Schuller, and Ralf Steinmetz
Multimedia Communication Lab (KOM)
Technische Universität Darmstadt
Darmstadt, Germany
e-mail: {firstname.lastname}@KOM.tu-darmstadt.de

***Abstract*—Today's cloud environments are very heterogeneous. This cloud heterogeneity, as the consequence of lacking cloud standards, builds technical and security barriers between cloud providers and blocks them from intended cloud collaborations within cloud marketplaces. A cloud broker, who acts on behalf of cloud providers, matches compatible collaborative partners according to their requirements and attempts to support the optimal exchange of cloud resources between them. The fulfillment of security requirements in cloud collaborations usually involves providing risk assessments, which are still very time-consuming and not applicable for ad hoc cloud collaborations within cloud marketplaces. Aiming to design and develop a security model for trading with cloud services, we identify in this paper concepts, mechanism and available tools that can support establishing of security-aware cloud markets. Furthermore, we introduce our information security governance driven cloud brokerage model with security labeling of tradable cloud products that can be the next step in the standardization process of tradable cloud products and optimize the selection of collaborative cloud partners.**

Keywords-cloud computing security; cloud collaborations; cloud brokerage; information security governance; risk assessment; cloud certification; security labeling

I. INTRODUCTION

Today's cloud environments are built up of heterogeneous landscapes of independent clouds. The heterogeneity of clouds, as a consequence of still nonexistent technology, security and audit standards, presents a hurdle for a proper collaboration between clouds, necessary for the building of the cloud ecosystem and cloud marketplaces [1].

The reasons for cloud collaborations can be very different: enterprise acquisitions, storage and compute power extensions, disaster recovery plans, sub-contracting and service outsourcing, the necessity for a wider spectrum of services, etc. Such cloud collaborations bring cloud providers further advantages. Besides the eco-efficiency, due to shared usage of data centers and technologies [2], a better scalability and cost reduction can be achieved by the ad hoc selling of free resources and buying of additional external resources. This exchange of cloud resources forms the basis of the cloud brokerage service model [3].

Cloud brokerage enables cloud providers to find an optimally suitable match for each other, i.e., to find a collaborative partner that meets all requirements of intended cloud collaboration. These requirements may include business aspects (pricing, timelines), technical aspects (compatibility, interoperability, availability), and of course legal and security aspects (level of data protection, security measures, compliance with different industrial regulations, etc.) [3, 4, 5]. The cloud broker is the leading actor in the cloud brokerage service model, and acts as a mediator between cloud service providers and cloud service consumers, providing matchmaking, monitoring and governance of cloud collaborations [6]. The matchmaking of security and legal requirements and especially monitoring of their fulfillment during the cloud collaboration is not trivial.

The security risks tend to accelerate by entering into cloud collaborations within cloud marketplaces, because collaborative partners may have different implemented security policies and standards [7]. Therefore, two main requirements must be met to provide secure and compliant cloud collaboration - the cloud broker must perform an optimally reliable security risk assessment prior to the collaboration, or on-demand; and the cloud broker must provide the security governance during the collaboration.

The security risk assessments of cloud providers are widely discussed in the recent research, but, to the best of our knowledge, these assessments are still very time-consuming and cannot be applied to ad hoc cloud collaborations [8].

In our research, we aim at the development of an efficient secure brokerage model, which can be used by the cloud broker in ad hoc cloud collaborations as well.

The remainder of the paper is organized as follows. In Section 2, we discuss the current cloud market environments and their supervision. Furthermore, we define types of cloud collaborations. Section 3 provides an overview of information security governance mechanisms in cloud collaborations with their advantages and disadvantages. In Section 4, we outline steps of our information security governance driven cloud brokerage model and propose our initial security labeling approach for tradable cloud products as a solution for secure ad hoc cloud collaborations. Section 5 gives an overview of related work. Finally, Section 6 describes our future work.

II. SUPERVISION OF CLOUD COLLABORATIONS WITHIN CLOUD MARKETPLACES

The current cloud market environments consist of heterogeneous clouds, cloud providers who sell services, customers who buy services, and cloud brokers who try to find *the perfect match* for their clients. In other words, cloud

markets present the aggregate of possible buyers and sellers of cloud services and cloud resources and the transactions between them that need to be controlled and properly supervised [9]. But the current cloud markets are not organized and supervised on the desired level, e.g., in comparison to financial or energy markets [10]. The financial markets are supervised by exchanges or other organizations that facilitate and oversee the trade, using physical locations (e.g., New York Stock Exchange (NYSE), Deutsche Börse (German Stock Exchange in Frankfurt), or European Energy Exchange (EEX) in Leipzig), or electronic systems (e.g., NASDAQ (National Association of Securities Dealers Automated Quotations), XETRA (Xchange Electronic Trading)). These are also regulated by different national and international authorities, e.g., U.S. Securities and Exchange Commission, Monetary Authority of Singapore, Energy Market Authority (EMA) in Singapore, Energy Community (EC) in Europe, etc [11]. Lack of control or supervision is one of main concerns of cloud collaborations within cloud marketplaces. The development of supervision approaches for the current cloud marketplaces, to provide *a fair and orderly cloud market*, is still at an embryonic stage. We propose the trading of cloud resources within predefined cloud collaborations as an interim solution to provide desired supervision and information security governance [9].

In [7] we identified three types of cloud collaborations with respect to the security critical areas: federated collaborations, loosely-coupled collaborations and ad hoc collaborations (as shown in Fig. 1) and examined their security issues and risks according to the following critical areas: legal risks, 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, insufficient monitoring and incident response, portability risk, and insufficient information security governance.

Security requirements, relevant for cloud partners within each collaboration type, must be fulfilled to enter a collaboration and become a right to trade.

A. *Federated collaborations*

A federated collaboration assumes the usage of a so-called *metapolicy*, which includes all policies of all collaborative clouds. This metapolicy reduces the possibility of the occurrence of security incidents and breaches, as all security configurations and controls are fully pre-agreed between collaborative partners. But it may also be *a single point of failure*, since if any incident occurs; it will affect all collaborative partners (as they all have the same level of protection). Additionally, such type of collaboration does not support *autonomy* and cloud providers can lose their so-called *unique selling points* (USPs). Establishing of and agreeing on the metapolicy is very time-consuming and can be also compared with the *over-the-counter* (OTC) trading or with *a bilateral negotiation.*

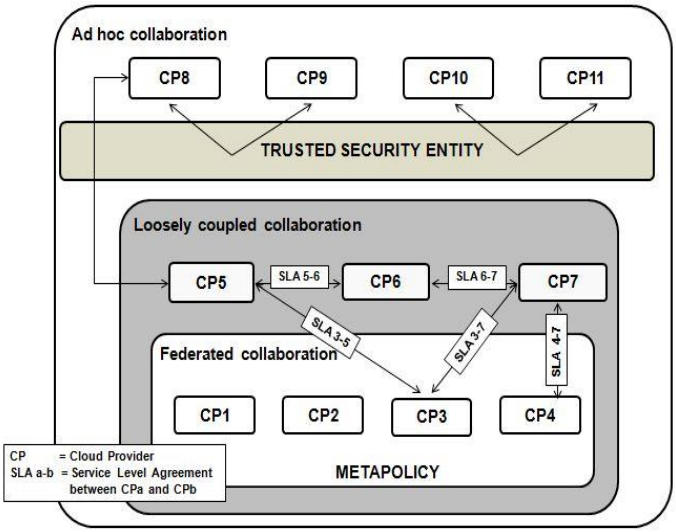

Figure 1. Types of cloud collaborations and trade-offs between them

B. *Loosely-coupled collaborations*

Loosely-coupled collaborations are more flexible and cover smaller (or regional) cloud environments, e.g., the European Union, the USA, Canada; or industry specific, e.g., financial or medical institutions. In this case, country or industry specific regulations, or *service level agreements* (SLAs) can be used as a basis for their security policies. Such geographical or industry-specific regulatory requirements allow to group cloud providers and apply shared security controls for more efficient management of the security environment (e.g., as in a community cloud).

C. *Ad hoc collaborations*

Ad hoc collaborations do not presume any kind of pre-agreed security policies or SLAs, the signing of which can be very time-consuming and can hamper the dynamic of data transfer and service delivery. The security check must be provided ad hoc as well, or in the nearly real-time Ad hoc collaborations are the most critical ones and cannot be performed without a proper supervision and information security governance over them in the form of *a trusted security entity* (e.g., cloud broker, identity broker, etc.).

In our research, we focus on ad hoc cloud collaborations within cloud marketplaces, those security concerns and possible information security governance solutions that can support the establishment of a fair and orderly cloud market.

III. INFORMATION SECURITY GOVERNANCE IN CLOUD COLLABORATIONS

In this section, we discuss the role of information security governance in cloud computing. Moreover, we outline information security governance mechanisms for different cloud collaborations identified in [7] with their *pros* and *cons*.

Security issues are very critical in cloud computing [4]. Many aspects must be examined concerning security risks in the cloud paradigm: legal risks, data privacy and data protection risks, users' and providers' security levels, right to audit and information security governance processes.

Information Security (IS) governance is a significant part of corporate governance in an enterprise and strives towards the understanding of the criticality of information security, endorsing the development and implementation of security programs and their alignment with business strategy. IS governance also takes the responsibility for performance management, reporting and risk management. In cloud computing, the role of IS governance has become enormously important, as enterprises deal with outsourced off-premise services with the involvement of diverse vendors and non-enterprise employees, whose compliance and activity must be monitored and reported [12, 13].

To the best of our knowledge, there are three security mechanisms to provide security governance over cloud providers [7]: cloud certifications, cloud risk assessments, and trusted security entities. Table 1 lists the current security mechanisms for each type of described cloud collaborations.

A. Cloud certification

Cloud certification sounds very promising and gives a certain sense of trust. The most cloud certificates are based on best practices security frameworks and already existing security standards, such as ISO (International Organization for Standardization), NIST (National Institute of Standards and Technology), CSA (Cloud Security Alliance) and FISMA (Federal Information Security Management Act). Many countries are trying to provide their own cloud certification or accreditation authorities and programs, such as TrustedCloud in Germany, Governmental Cloud in the USA, EuroCloud in the EU. The main disadvantage of cloud certification is its *generality*. These certificates are not always sufficient for peculiar cases (e.g., for critical data, banking transactions, country laws) and should be adapted or extended with other security governance mechanisms (e.g., risk assessments, security policies and audit).

B. Cloud risk assessments

Cloud risk assessments are more granular and can be used with respect to different industries (banking, insurance, healthcare). Cloud risk assessments are also based on the existing risk assessments and are extended with specific vendor governance controls for availability, auditing and accountability. These risk assessments are provided by ISO, CSA, BSI (Bundesamt für Sicherheit in der Informationstechnik, Federal Office of Information Security in Germany), and ENISA (European Network and Information Security Agency), COBIT (Control Objectives for Information and Related Technology), ISACA (Information Systems Audit and Control Association), Basel Accords, and SOx (Sarbanes-Oxley Act).

The risk assessment process is very time-consuming and mostly cannot be automated. Furthermore, in case of risk acceptance procedures or a necessary risk remediation, can be followed by numerous expensive complex bilateral agreements.

TABLE I. IS GOVERNANCE MECHANISMS IN CLOUD COMPUTING

IS governance mechanism	**Type of cloud collaboration**		
	Federated	***Loosely-coupled***	***Ad hoc***
Cloud certification	Proprietary, Best practices	ISO 27000 [14], NIST [15], EuroCloud [16], CSA [12], NIST-FISMA [17]	As in loosely-coupled, but with sufficient evidence
Cloud risk assessement (RA)	Proprietary, Best practices	ISO 27000 [14], Shared program [18], ENISA Audit [19], CSA RA [24], BSI Guidelines [12], ISACA RA [21], CObIT [22], Basel II [4], Basel III [4], SOx [20], Cloud-Leitstand [25]	As in loosely-coupled, but with sufficient evidence
Trusted security entity	Not needed or Auditors [13], Lawyers [22]	Auditors [13], Lawyers [22], Security experts	Identity federation broker [26], Identity cloud agent [27], Identity as a Sevice [28], Security as a Service [7], SAML [26], Data access frameworks [27], Data labeling [28], Trusted platform modules [29], Single-sign-on [30]

C. Trusted security entity

A trusted security entity concept is more dynamic, but currently does not cover all security aspects of cloud computing. It is mostly focused on identity and access management, ignoring infrastructure, network, and application security.

The existing solutions, especially for ad hoc collaborations, do not cover the whole aspects of cloud security or need sufficient evidence for their implementation, e.g., monitoring and logging tools in place, or regular auditing. Some legal aspects can be outsourced to such trusted entities (authorities) that can assume the liability and responsibility.

To combine all the security aspects of cloud security and enable auditing and controlling of their fulfillment, a new, *"information security governance driven"* solution is needed.

IV. An Information Security Governance Driven Cloud Brokerage Model

In this section, we present our initial IS governance driven cloud brokerage model as a new trusted security entity solution for cloud marketplaces.

To start with, we examine the main features of the established stock exchange brokerage model [31] and use them to identify initial requirements on our IS governance driven cloud broker and its functionality, which we define as follows:

1) The IS governance driven cloud broker (ISGDCB) brings cloud providers together and facilitates a secure collaboration between them;

2) The ISGDCB should include a full range of services necessary to cover the information security governance process - risk assessments, risk analysis, negotiations of security protection level agreements (SPLA), auditing and controlling of their fulfillment;

3) The IS governance process should be dynamic and with a low latency;

4) Any bilateral communication between cloud providers should be avoided, it should take place only via the ISGDCB;

5) The ISGDCB must be cloud provider independent, to avoid the so-called vendor lock-in effect;

6) The ISGDCB should be applicable for the "Everything as a Service" model.

On the basis of the described requirements, we suggest our IS governance driven cloud brokerage model, which consists of four modules: Pre-Governance, Collaboration, Governance, and Post-Governance.

A. Module 1 - Pre-Governance

In this module, the ISGDCB defines a secure framework for a regulated collaboration between cloud providers. Three approaches can be used here:

Approach 1 – ISGDCB creates and provides a risk assessment for cloud providers to classify their security level and criticality. This risk assessment must include all critical areas of cloud collaborations (legal and risk aspects, data protection policies, regulator's requirements for special countries and industries, etc.) [12]. The results of risk assessments in the form of cloud provider's labeling are then stored in the assessment database (AD) and used in the Module 2. The cloud providers' labeling must be sufficient and up-to-date to make a proper provider selection for a potential collaboration. Recent research work shows that cloud provider labeling based on risk assessment results is very time-consuming and often very subjective, as security controls and security attributes are qualitative (and not quantitative) in their nature [10]. Therefore, we suggest Approach 2 to optimize this process step.

Approach 2 – ISGDCB performs the security labeling (in addition to the technical specification) of all tradable products according to their security features: type of service (storage, application, database, etc.), geographical restriction, level of segregation, data protection criticality, related monitoring requirements (services), authentication, identity and accountability mechanisms, network security and encryption mechanisms, etc. This labeling should be granular enough to depict all compulsory data protection laws and regulatory policies related to the countries, where the products will be sold or bought.

Approach 3 – ISGDCB provides both *Approach 1* and *Approach 2*, which can give a more transparent view of the whole security framework and establish a stronger regulated cloud market. But this approach is more time-consuming and it makes sense to apply it only to high critical cloud products, e.g., databases with personal data.

B. Module 2 – Collaboration

In this module, cloud providers send their collaboration requests for buying or selling of products to the ISGDCB. The ISGDCB matches the cloud providers' labeling (if needed also products' labeling) using the assessment database (AD) and let the "security compatible" cloud providers collaborate.

C. Module 3 – Governance

The relevant IS governance processes must be established in this module. The ISGDCB monitors and regulates the fulfillment of these IS governance processes by cloud providers during their collaborations. To monitor IS governance processes, proper security protection level agreements (SPLA) must be set for each type of collaboration. SPLAs include the roles and responsibilities of the collaborative cloud providers, timelines, event-based patterns, penalties in case of any SPLA violations, and the incident response management process.

The definition of the event-based patterns for the monitoring is not trivial. The ISGDCB must know *what* must be monitored in the real-time and *how* to use these events optimally to detect any violations and provide the relevant incident response to report and (if possible) remediate occurring violations.

D. Module 4 – Post-Governance

The ISGDCB stores, checks and reports the logging and auditing information of the IS governance processes and cloud collaborations to comply with accountability

requirements and for eventual forensic investigations. The ISGDCB can provide collaborative cloud providers with auditing or logging information, if this requirement was pre-agreed.

We suppose that our proposed initial IS governance driven cloud brokerage model can optimize the selection of collaborative partners. Furthermore, we believe that our security labeling approach can be the next step in the standardization process of tradable cloud products. Our model can be applied to all types of cloud collaborations within cloud marketplaces.

V. Related Work

Collaboration among cloud providers with respect to security and privacy is widely discussed in the recent literature.

Xin and Datta [32] explore how the social factor "trust" can enable cloud providers' collaborations in decentralized setting to complement their resource. The authors propose a framework, based on Dirichlet distribution, which combines disparate trust information - from direct interactions and from (indirect) references among service providers, as well as from customer feedbacks. Using such information service providers decide whether to initialize collaborations by selecting trustworthy partners. Technical parameters, security check are not considered in their work.

Almorsy, Grundy, and Ibrahim [33] introduce a cloud security management framework based on aligning the FISMA standard to fit with the cloud computing model, enabling cloud providers and consumers to be security certified. This framework is built on top of a number of security standards that assist in automating the security management process. The automation is based on the results of risk assessments that are compared to the service descriptions. The authors cover only technically measurable results for the scoring and do not use labelling.

Nair et al. [34] propose a cloud bursting and cloud brokerage model to broker between multiple cloud providers and to aggregate them into composite services. The models are based only on the identity access management (IAM) namely, user credentials, to verify their identity.

Tossi et al. [35] explore in their research Cloud Federations, a recent paradigm that enables outsourcing requests to other federation members for IaaS providers in order to avoid spikes and become cheaper VMs. The authors propose policies that help in the decision-making process to increase resources utilization, fulfillment of QoS requirements, and profit in a Cloud federation environment. Security policies are not yet considered in their work.

Nguyen et al. [36] introduce the Monterey Security Architecture (MYSEA), which addresses the need to share high-value data across multiple domains of different classification levels while enforcing information flow policies. This architecture allows users with different security authorizations to securely collaborate and exchange information using commodity computers and familiar commercial client software that generally lack the prerequisite assurance and functional security protections. MYSEA seeks to meet two compelling requirements: enforcing critical, mandatory security policies, and allowing access and collaboration in a familiar work environment. Recent additions to the MYSEA design expand the architecture to support a cloud of cross-domain services, hosted within a federation of multilevel secure servers. This model maintains the federated control necessary to support and protect cross-domain collaboration within the enterprise. The resulting architecture shows the feasibility of high-assurance collaboration, but not in the context of trading.

To the best of our knowledge, we are the first who explores the building of cloud collaborations in the context of traiding with cloud resources undder fulfillment of information security requirements.

VI. Conclusion and Future Work

In our work, we gave an overview of the types of cloud collaborations from the security perspective and outlined the role of the IS governance in the cloud collaborations.

We also described advantages and disadvantages of the existing IS governance mechanisms – cloud risk assessments, cloud certifications, and trusted security entities.

Furthermore, we proposed our IS governance driven cloud brokerage model, which can bring more dynamic in cloud collaborations by using security labeling of tradable cloud products instead of requiring long lasting negotiations and assessment processes on the cloud providers' side. The ISGDCB takes over this role, ensures the quality of related IS governance processes, and provides transparency to collaborative cloud providers.

Our future work aims at the technical implementation and simulation of our IS governance driven cloud brokerage model to identify and improve its weak points. Furthermore, we plan to analyze security labeling mechanisms for tradable products and their requirements to provide a proper security framework for the Pre-Governance module. Our security labeling for cloud products can support the standardization of cloud products and cloud markets, which is necessary for the building of the secure cloud ecosystem.

Our next challenge is the definition and technical implementation of event-based patterns to establish an optimal real-time monitoring of the IS governance processes and detection of occurring security breaches and violations during ad hoc collaborations within cloud markets.

Acknowledgment

This work is supported in part by E-Finance Lab e. V., Frankfurt am Main, Germany (http://www.efinancelab.com).

REFERENCES

[1] Kretzschmar, M., Golling, M.: Security management spectrum in future multi-provider Inter-Cloud environments - Method to highlight necessary further development. In: 5th International DMTF Academic Alliance Workshop on Systems and Virtualization Management (SVM), pp. 1-8 (2011)

[2] Guitart, J., Torres, J.: Characterizing Cloud Federation for Enhancing Providers' Profit. In: IEEE 3rd International Conference on Cloud Computing (CLOUD), pp. 123-130 (2010)

[3] Uttam Kumar, T., Wache, H.: Cloud Broker: Bringing Intelligence into the Cloud. In: IEEE 3rd International Conference on Cloud Computing (CLOUD), pp. 544 – 545 (2010)

[4] Lampe, U., Wenge, O., Müller, A., Schaarschmidt, R.: Cloud Computing in the Financial Industry - A Road Paved with Security Pitfalls? In: 18th Americas Conference on Information Systems (AMCIS), Association for Information Systems (AIS), (2012)

[5] Siebenhaar, M., Wenge, O., Hans, R., Tercan H., Steinmetz, R.: Verifying the Availability of Cloud Applications. In: 3rd International Conference on Cloud Computing and Services Science (CLOSER 2013), accepted for publication

[6] Gomes, E., Vo, Q.B., Kowalczyk, R.: Pure exchange markets for resource sharing in federated clouds. In: Concurrency and Computation: Practice and Experience, Vol. 24, Issue 9, pp. 977–991 (2012)

[7] Wenge, O., Siebenhaar, M., Lampe, U., Schuller, D., Steinmetz, R.: Much Ado about Security Appeal: Cloud Provider Collaborations and their Risks. In: 1st European Conference on Service-Oriented and Cloud Computing (ESOCC), Springer, pp. 80-90 (2012)

[8] Schnjakin, M., Alnemr, R., Meinel, C.: Contract-based cloud architecture. In: Iternational workshop on Cloud data management (CloudDB), pp. 33-40 (2010)

[9] Garg, S.K., Vecchiola, C., Buyya, R.: Mandi: a market exchange for trading utility and cloud computing services. In: Springer Science+Business Media, (2011)

[10] Garg, S.K., Versteeg, S., Buyyaa, R.: A framework for ranking of cloud computing services. In: Future Generation Computer Systems, Vol. 29, Issue 4, pp. 1012–1023 (2013)

[11] Rahimi, A.F., Sheffrin, A.Y.: Effective market monitoring in deregulated electricity markets. In: IEEE Transactions on Power Systems, Vol. 18, Issue 2, pp. 486 – 493 (2003)

[12] CSA, https://cloudsecurityalliance.org/research/security-guidance

[13] SIT Technical Report, On the Securityof Cloud Storage Services (2012)

[14] ISO, http://www.iso.org/iso/catalogue_detail?csnumber=42103

[15] NIST report, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[16] EuroCloud, http://www.eurocloud.org/tag/certification/

[17] Wood, K., Anderson, M.: Understanding the complexity surrounding multitenancy in cloud computing. In: IEEE International Conference on e-Business Engineering, pp. 119 – 124 (2011)

[18] SA, http://sharedassessments.org/media/pdf-EnterpriseCloud-SA.pdf

[19] ENISA, http://www.enisa.europa.eu/activities/

[20] Yang, D.: Ad Hoc Aggregation Query Processing Algorithms Based on Bit-Store. In: International Conference on in Data Intensive Cloud Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), pp. 313 – 320, (2011)

[21] ISACA Information Security Governance Guidance for Boards of Directors and Executive Management, 2006, http://www.isaca.org/

[22] COBIT, Knowledge-Center/COBIT/Pages/Overview.aspx

[23] Bernstein, D., Vij, D.: Intercloud Security Considerations. In: IEEE International Conference on Cloud Computing Technology and Services, pp. 537 – 544 (2012)

[24] Bernsmed, K., Jaatun, M.G, Meland, P.H., Undheim, A.: Security SLAs for Federated Cloud Services. In: International Conference on Availability, Reliability and Security, pp.202 – 209 (2011)

[25] AISEC Fraunhofer Leitstand Project, http://www.aisec.fraunhofer.de/content/dam/aisec/de/pdf/problas/

[26] Papish, M.: A method for implementing dynamic, cloud-based metadata services based on a unified content ID space cross a fragmented CE ecosystem. In: IEEE International Conference on Consumer Electronics (ICCE), pp. 57 – 60 (2012)

[27] He., Y.H., Bin, W., Xiao, X.L., Jing, M.X.: Identity Federation Broker for Service Cloud. In: International Conference on Service Sciences, pp. 115 – 120 (2010)

[28] Ates, M., Ravet, S., Ahmat, A., Fayolle, J.: An Identity-Centric Internet: Identity in the Cloud, Identity as a Service and other delights. In: International Conference on Availability, Reliability and Security, pp. 555 – 560 (2011)

[29] Goyal, P.: Application of a Distributed Security Method to End-2-End Services Security in Independent Heterogeneous Cloud Computing Environments. In: IEEE World Congress on Services (SERVICES), pp. 379 – 384 (2011)

[30] OASIS-Security-Services, https://www.oasis-open.org

[31] Corporation Essvale Corporation Limited, "Business Knowledge for It in Prime Brokerage", 2008

[32] Xin, L., Datta, A.: On trust guided collaboration among cloud service providers. In: 6th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), pp. 1-8 (2010)

[33] Almorsy, M., Grundy, J, Ibrahim, A.S.: Collaboration-Based Cloud Computing Security Management Framework. In: IEEE International Conference on Cloud Computing (CLOUD), pp. 364 - 371 (2011)

[34] Nair, S.K., Porwal, S., Dimitrakos, T., Ferrer, A.J., Tordsson, J., Sharif, T., Sheridan, C., Rajarajan, M., Khan, A.U.: Towards Secure Cloud Bursting, Brokerage and Aggregation. In: IEEE 8th European Conference on Web Services (ECOWS), pp. 189 - 196 (2010)

[35] Toosi, A.N., Calheiros, R.N., Thulasiram, R.K., Buyya, R.: Resource Provisioning Policies to Increase IaaS Provider's Profit in a Federated Cloud Environment. In: IEEE 13th International Conference on High Performance Computing and Communications (HPCC), pp. 279 – 287 (2011)

[36] Nguyen, T.D., Gondree, M.A., Shifflett, D.J., Khosalim, J., Levin, T.E., Irvine, C.E.: A cloud-oriented cross-domain security architecture . In : Military Communications Conference (MILCOM), pp. 441 - 447 (2010)