Functional components for a Security Manager within future Inter-Cloud environments

Michael Kretzschmar and Mario Golling
Universität der Bundeswehr München
Faculty of Computer Science
D-85577 Neubiberg, Germany
Email: {michael.kretzschmar and mario.golling}@unibw.de

***Abstract*—Especially in the public sector, great efforts can be seen towards the Inter-Cloud (e.g., USA Federal Government's Cloud Computing Initiative). In order to make a contribution towards the challenges of security management in Cloud Computing respectively Inter-Cloud, this paper focuses on the identification of functional components for a Security Manager. Therefore, we present identified functional components (basic function and process components) for a Security Manager architecture. These components together with identified security data artifacts will support the Cloud provider community to implement a security management system, and facilitate the adoption of this results in the private and public sector. As a first step towards this, we present a detailed and comprehensive analysis of the security management functional components within current Cloud approaches, which can serve as a basis for future developments towards Inter-Cloud environments.**

***Keywords*-Security Manager, Cloud Security Management, Inter-Cloud, DMTF Cloud Service Reference Architecture**

I. Introduction and Status Quo

Inadequate solutions for security management challenges can be the show-stopper for ubiquitous Cloud computing usage, as Cloud computing services multiply and expand faster than the ability of Cloud computing consumers to manage or govern their usage [1], [2], [3]. Especially the evolution of Cloud computing towards Inter-Cloud environments (also driven by governmental and military efforts within the public sector [4], [5], [6]) makes these challenges even more complex [7].

The Inter-Cloud [8] as 'an interworking of Cloud systems of different Cloud providers' accelerates the erosion of trust boundaries already happening in organizations [9], [10], [11], [12]. In addition, a provider in an increasingly complex and distributed Inter-Cloud environment has the need for a consistent overview about security management components that guides future implementation and adaption within his Cloud system [13], [14], [15].

The so called Security Manager element within the generic Distributed Management Task Force (DMTF) Cloud Reference Architecture (CRA) can serve as a basis for implementing and adapting a concrete Cloud system [16]. But DMTF mainly describes their elements only as black boxes. Therefore, the generic DMTF CRA of a Cloud system has to be mapped to the Inter-Cloud context in order to adapt and extend requirements for the Security Manager (SM) element, that represents all security management related aspects, functions and processes within the Cloud system of a provider [16], [17], [18]. In addition, well-established security management approaches (like Enterprise Security Management (ESM)) have to be considered and - for instance in the case of the public sector - they are sometimes even mandatory [19], [20], [21], [22]. Furthermore, there are several sources that describe Cloud computing security areas [23], [24], [25]. However, they differ in defining and covering necessary security management functional areas and interaction aspects that can be used for a comprehensive Cloud security management compared to traditional approaches. Based on the requirements and the security management approaches, we identify necessary functional components (basic function and process components) for a future Security Manager architecture [25]. On the one hand, these components may guide the adaption and functional homogeneity of a SM within existing providers. On the other hand a new provider can use currently available Cloud service offerings and standards for implementing his specific Cloud system.

The short paper is structured as follows. In Section II, we provide key facts about the Inter-Cloud environment as well as an overview of the DMTF CRA setting - the environment for the Security Manager. Following this, in Section III designed aspects for a SM are presented which are derived from a wide spectrum of examined Inter-Cloud use cases. These aspects are fulfilled through functions and processes, which are clustered into functional and process components for a SM. Current Cloud services are analyzed regarding there coverage of the identified functional components in Section IV that concludes this paper.

II. Security Manager Environment

A. The Inter-Cloud environment

An Inter-Cloud is defined as a 'Cloud model that, for the purpose of guaranteeing service quality, such as the performance and availability of each service, allows on-demand reassignment of resources and transfer of workload through an interworking of Cloud systems of different Cloud providers based on coordination of each consumer's requirements for service quality with each provider's Service Level Agreement (SLA)' [13], [26]. Security parameters such as location of

978-1-4577-1811-3/11/$26.00

Cloud service, encryption of consumer data, status of provider certification, etc. are part of this SLA.

A single Cloud system is represented by his provider and can be mapped to one ore more organizations. The provider has to fulfill security requirements towards their consumers and other providers. Each provider in the Inter-Cloud is an autonomous enterprise and federates with other providers based on his own local preferences governed by policies that are aligned with its business goals [27]. The Inter-Cloud aims to cooperate applying Cloud services and all the related procedural Cloud services from multiple independent providers in such a way that the consumer can see all the services involved as one service [13]. Therefore, a Cloud provider is able to transparently enlarge its own Cloud resources amount using further computing and storage capabilities from other Cloud systems [13], [16].

B. DMTF Cloud Reference Architecture

In contrast to Section II-A, where the different providers are mainly seen as a black box, [16] proposes three generic elements for one specific provider within the DMTF CRA. The element *(1) Cloud Infrastructure* refers to the actual runtime environment, where all the Cloud services are really executed. Here, the instantiation of a Cloud service is called *Cloud Service Instance*. It specifies one concrete expression of a service and consists of one ore more *Service Topology Items*.

The management tasks of a provider are summarized in the *(2) Cloud Management*. It consists of three management components. Generally, a *(2a) Service Catalog* is a database of information about the Cloud services offered by a service provider. The service catalog mainly includes (i) a description, (ii) the type of service, (iii) support costs, (iv) agreed SLAs, and (v) consumer information. The management of the Cloud service instance and service topology items is done by the *(2b) Service Manager*. He provides the means to create, change or delete these instances including monitoring, and control at runtime. Finally, the *(2c) Security Manager* is responsible for the management of the Cloud infrastructure according to specified security requirements.

Within the management domain a *(3) Data Artifact* describes an information object or logical representations of provider objects, such as consumers and provider policies. These data artifacts are managed by the Cloud management and used in order to transfer information between intra- and inter-provider components. The following basic data artifacts are presented in DMTF CRA. The collection of items (like machine images, connectivity definitions and storage) that is stored in the service catalog and that can be provisioned at the Cloud service provider is the *(3a) Service Template*. A unique, distinct, and measurable aspect of an SLA is a *(3b) Service Level Objective (SLO)*. Through the use of an *(3c) SLA*, all parties must agree that sets of SLOs. The combination of a service template and an SLA is called a *(3d) Service Offering* and will be instantiated as a Cloud service instance.

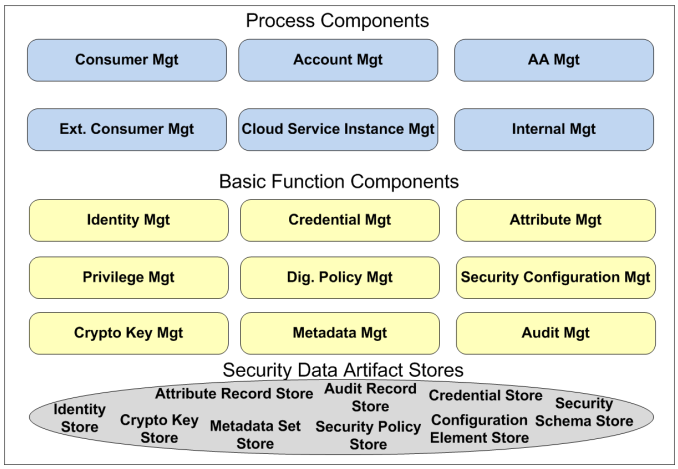

Figure 1. Functional components of a Security Manager with their managed security data artifacts

III. Components for a Security Manager

A. Genesis of the identified components

The presented components of a SM within the next paragraph are identified, described and modeled based on the following methotology and research work. First of all we collected various Inter-Cloud use cases and scenarios within the private and public sector (e.g. EDA's Military Cloud [4]). Based on this a comprehensive list of requirements focusing security management could be identified for the Security Manager [28]. In order to fulfill these requirements we derived a set of basic functions and processes for security management of Inter-Cloud providers together with related data artifacts (such as a credential, consumer account, etc.). Where a basic function represents an atomic activity within the SM itself that creates, modifies or deletes data artifacts. In contrast, a process represents a more complex workflow interoperating basic functions in order to interact with the environment of the SM (intra-provider, extra-providers and consumers). Consequently a process does not edit a data artifact. Afterwards, we clustered these functions and processes within nine basic function components and six process components that will form the internal architecture of a future SM. This architecture can be used to guide the implementation or extension of a specific SM within a concrete Cloud system of a provider within the future Inter-Cloud (described in section II-A).

B. Components description

This paragraph presents the (1) basic function and (2) process components, as well as the (3) stores for identified data artifacts of a SM architecture (visualized in Figure 1). Each component contains the identified basic functions respective processes. Due to space limitation, we describe the components in total.

1) Basic Function Components: A basic functional component includes functions that belong to the same security management field. In addition, the clustering of basic functions in components is done according to managed data artifacts. The nine basic functional components are described

as follows:
Identity Management is the ability to confirm and manage the life-cycle of an assured identity (consumer, Cloud service instance, service user, etc.). This identity can be provider internal or derived from other providers (e.g., an identity of an external Cloud service instance). Federated Identity Management provides end users with secure access across multi-provider Cloud services through federated single sign-on.
Credential Management is the ability to manage the life-cycle of digital credentials (that are bound to an identity). Examples of credentials include certificates, identification documents, passwords and keys. The credential management is also responsible for verifying the authenticity of credentials.
Attribute Management is the ability to manage the assigned attributes, where an attribute is a specification which defines a property of an identity, within an attribute record. This includes the management of the life-cycle of an attribute record for specific identities as well as the maintenance of attribute record templates. The templates are used to instantiate attribute records.
Privilege Management is the ability to manage permissions to perform an action (e.g., providing role management and separation of duties for access control of Cloud service instances).
Digital Policy Management is the ability to generate, convert, manage and replace digital policies. Digital policies are in machine-specific languages and can be used to guide the behavior of systems in an automated or semi- automated manner. According their purpose these policies can be clustered into policies for authorization or configuration.
Security Configuration Management manages security-related configuration items (such as defining, controlling, ordering, and loading of configuration data) for Cloud service instances and service topology items of the provider. The SLO are guarantied by using these configuration items for the instantiation of Cloud services. In addition this component manages security services (e.g. transport encryption services, firewalls, etc.) that can be used by any provider component in order to support data isolation for multi-tenant storage and separation of consumer data from operational data.
Cryptographic Key Management encompasses all of the activities involved in the handling of cryptographic keys during the entire life-cycle of the keys.
Metadata Management is the ability to generate and manage all security-relevant metadata sets binded to an object and values over their life-cycle in order to define the handling of objects. This includes the transfer of security requirements into SLO which in turn create the basic for SLA within the service offering.
Audit Management is the ability that establishes security-relevant audit events which lead to the monitoring of service behavior from a security perspective. This allows in turn the analysis and report of current and former situations leading to security situational awareness. In addition audit management is the ability to gather and manage security-relevant information of Cloud service instances (such as data location, sub-provider usage, etc.).

2) Process Components: A process component contains processes, that represents a more complex workflow of interoperating basic functions in order to interact with the environment of the SM. These processes are clustered according their tasks and interaction focus (e.g., intra-provider, external to other providers, consumers, etc.).
Consumer Management is the ability to support security management operations between the consumer and the provider. This includes operations for maintaining credentials of the consumer to authenticate him in different roles, as well as the configuration of privileges for the usage of his Cloud service instances. In addition, the consumer is supported by processes for audit report generation and compliance analyses.
External Consumer Management is the ability to support security management operations of the provider at other providers. The component contains processes similar to Consumer Management.
Cloud Service Instance Management is the ability to provide necessary security processes while creating, changing or deleting Cloud service instances (e.g., external Cloud service instances for disaster recovery and backup). This includes internal or external Cloud service instances.
Account Management is the ability to provide processes to maintain accounts for consumers and providers (e.g., accounts for migration, hot-standby, service users, etc.). This also includes processes for the registration and de-registration of consumers.
Authentication and Authorization Management is the ability to provide processes to authenticate a consumer concerning a specific role and authorize him for role related actions. In addition this component contains processes that support the access of the provider at other providers (e.g., the login to use or manage a Cloud service instance of an other provider).
Internal Management is the ability to provide processes to transfer security requirements into consistent configured Cloud service instances in support of the security administrator.

3) Security Data Artifacts Stores: Security data artifacts of the same security management field are grouped and stored within so called *Security Data Artifacts Stores*. Within Figure 1 nine stores are presented that represent the sets of identified security related data artifacts.

IV. Analysis of Cloud Security Management functions

In order to foster the move towards an interoperable security management for Inter-Cloud providers, it is necessary to analyze the status quo of security management within two chronological steps. First, the conformance of current approaches to the identified security management basic functions has to be determined. Afterwards necessary extensions or modifications of these functions can be addressed. In a second step, processes

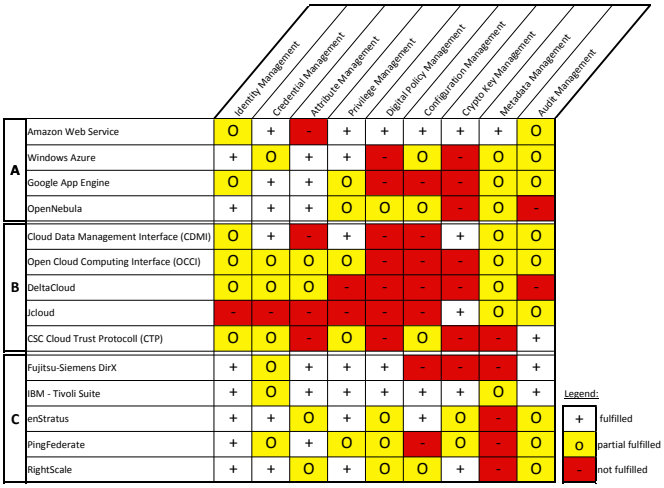

Figure 2. Coverage of functional components with included security management functions by current Cloud service offerings and standards

built upon these security management basic functions can be adapted towards Inter-Cloud activities.

In this section we briefly present the results (see Figure 2) of our analysis of fourteen Cloud service offerings and standards. In the following we describe the analysis of one Cloud service for a identified category and present the summarized results in the end.

A. Specific Cloud service provider API

Various Cloud service providers add security functions covering also some parts of Cloud security management to their proprietary Cloud service offerings. For example, Amazon Elastic Compute Cloud (Amazon EC2) supports a multi-factor authentication (knowledge and ownership) to gain access, control privileges, and support of credentials such as X.509 certificates or a proprietary Amazon Secret Access Key (e.g., to sign API calls). A key management allows the concurrent usage of these certificates respectively keys. Access is logged and audited. In addition, basic metadata functions such as creation, modification and deletion are offered. Furthermore, flexibility to place instances within multiple geographic regions as well as across multiple availability zones is possible, however the choice is limited (e.g., region, continent) [29], [30].

B. Standardized Cloud service provider API

Interfaces and APIs for Cloud portability and interoperability include management and security issues. For example, security in the context of Cloud Data Management Interface (CDMI) refers to the protective measures employed in managing and accessing data and storage. CDMI can be accessed by protocols like SAN, NAS, FTP, WebDAV or REST. Security management measures within CDMI can be summarized as user and entity authentication, authorization, access controls, data integrity, data at-rest encryption, crypto key management, auditing, and meta-data management [31]. The security management fields credential, privilege, and crypto key management fully cover the security management functions, whereas functions from other areas such as identity management are missing.

C. Security Management as a Cloud service

PingFederate is a Cloud-based Identity-as-a-Service provider that focuses on federated identity management and is integrated by a provider-specific API. These kinds of Cloud services can be assigned to Software-as-a-Service (SaaS). The Identity Provider sends identity attributes (from an authentication service or application) to PingFederate which forwards them to the target application of a service provider in order to provide single-sign-on to applications. PingFederate supports different access authentication credentials such as Windows IWA/NTLM, X.509 certificates, or LDAP Authentication Service. The initial user authentication is normally handled outside of the PingFederate [24], [32].

Summarized results

The results of our detailed analysis of fourteen Cloud service offerings covering the three categories are presented within Figure 2. In general, our evaluation criteria (fulfilled/partial fulfilled/not fulfilled) was guided by their conformance to the basic function components and the amount of basic functions included. In order to reach a common point of comparison for the evaluation we abstracted from various provider-specific implementations that have also minor functional differences between the same security management function. Various Cloud service providers like Amazon Web Services [33], Windows Azure [34], Google App Engine [35], OpenNebula [36], etc. implement specific security functions for their Cloud service offerings, covering mainly security management functions for authentication and authorization. As basic functions for Metadata and Audit Management are not implemented, it raises trust and risk management issues by their consumers. Standardized interfaces and APIs, such as CDMI [31], OCCI [37], DeltaCloud [38], JCloud [39], or CSC CTP [40] include less security management issues compared to specific Cloud provider offerings. Traditional security management systems such as Fujitsu-Siemens DirX [41] or IBM Tivoli Suite [41] support a wide range of necessary security management functions. An integration and adaption of their functions for Cloud computing providers is promising, but their focus on a unique organization with less federation and dynamic reconfiguration aspects raises new challenges within the second step towards Inter-Cloud environments. Finally, management and especially security management functions can be the main function of the Cloud service (e.g., enStratus, PingFederate [32], RightScale [42], etc.) itself. From an overall security management spectrum their range of security management functions is limited and often only interoperable with specific Cloud services (e.g. RightScale is only working for Infrastructure-as-a-Service (IaaS) Cloud service providers).

ACKNOWLEDGEMENT

This research activity has been supported partially in cooperation with the Federal Office for Information Security Germany.

REFERENCES

[1] R. Miller, "Cloud brokers: The next big opportunity?" Online, 2009. [Online]. Available: http://www.datacenterknowledge.com/archives/2009/07/27/Cloud-brokers-the-next-big-opportunity/

[2] N. Gruschka and M. Jensen, "Attack Surfaces: A Taxonomy for Attacks on Cloud Services," in *Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on*. IEEE, 2010, pp. 276–279.

[3] T. . GROUP, "Cloudscape - cloud codex," Online-Quelle, 2009, white Paper. [Online]. Available: www.451group.com/reports/executive_summary.php?id=869

[4] EDA PT CIS, "Collaboration in the cloud and challenges to cyber defence," EDA Whitepaper, 2010, European Defense Agency, EDA CAP KM CIS 2010.

[5] V. Kundra, "State of public sector cloud computing," U.S. Chief Information Officer, Report, Mai 2010.

[6] T. Greenfield, "Cloud computing in a military context - beyond the hype," Online-Quelle, 2009, dISA Office of the CTO. [Online]. Available: http://www.disa.mil/conferences/2009/briefings/cto/Cloud\%20Computing\%20in\%20a\%20Military\%20Context.ppt

[7] D. Bernstein and D. Vij, "Intercloud security considerations," *Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on*, pp. 537 – 544, 2010. [Online]. Available: http://ieeexplore.ieee.org/

[8] D. Bernstein, E. Ludvigson, K. Sankar, S. Diamond, and M. Morrow, "Blueprint for the intercloud-Protocols and formats for cloud computing interoperability," in *2009 Fourth International Conference on Internet and Web Applications and Services*. IEEE, 2009, pp. 328–336.

[9] S. Microsystems, "Take your business to a higher level - sun cloud computing technology scales your infrastructure to take advantage of new business opportunities," Online-Quelle, 2009, guide.

[10] A. Celesti, F. Tusa, M. Villari, and A. Puliafito, "How to Enhance Cloud Architectures to Enable Cross-Federation," in *2010 IEEE 3rd International Conference on Cloud Computing*. IEEE, 2010, pp. 337–345.

[11] D. Bernstein, E. Ludvigson, K. Sankar, S. Diamond, and M. Morrow, "Blueprint for the intercloud - protocols and formats for cloud computing interoperability," *Internet and Web Applications and Services, 2009. ICIW '09. Fourth International Conference on*, pp. 328 – 336, 2009. [Online]. Available: http://ieeexplore.ieee.org

[12] H. Sakai, "Introduction to global inter-cloud technology forum (gictf) and its roadmaps," Online-Quelle, 2009. [Online]. Available: http://www.gictf.jp/index_e.html

[13] GICTF White Paper, Global Inter-Cloud Technology Forum, 2010, "Use cases and functional requirements for inter-cloud computing," Online, 2010.

[14] C. Hoff, "The cloud magic 8 ball (future of cloud)," Online-Quelle, 2010, cloud Security Alliance Keynote. [Online]. Available: http://www.rationalsurvivability.com/blog/?s=jericho+forum

[15] M. Kretzschmar and S. Hanigk, "Security management interoperability challenges for collaborative clouds," *Systems and Virtualization Management (SVM), 2010 4th International DMTF Academic Alliance Workshop on*, pp. 43 – 49, 2010. [Online]. Available: http://ieeexplore.ieee.org/

[16] D. O. C. S. Incubator, "Architecture for managing clouds - a white paper from the open cloud standards incubator," Online-Quelle, 2010, version: 1.0.0 and Document Number: DSP-IS0102.

[17] ——, "Use cases and interactions for managing clouds - a white paper from the open cloud standards incubator," Online-Quelle, 2010, version: 1.0.0 and Document Number: DSP-IS0103.

[18] ——, "Dmtf cloud security mechanisms for provider interface," DMTF Dokumentation, 2010, version: 0.5 and Document Number: DSP1000.

[19] B. Farroha and D. Farroha, "Cyber security components for pervasive enterprise security management and the virtualization aspects," in *Systems Conference, 2010 4th Annual IEEE*. IEEE, 2010, pp. 553–558.

[20] NSA, "Enterprise security management: A context overview," 2009, nSA Documentation.

[21] European Defense Agency, "End-to-end security management in a heterogeneous environment," 2009, eDA 08-CAP-027.

[22] NATO, "Concept of a nato security management infrastructure," 2008, aC/322(SC/4-AHWG/3)WP(2007)0001).

[23] C. S. Alliance, "Security guidance for critical areas of focus in cloud computing v2.1," 2009.

[24] J. Rhoton, "Cloud computing explained: Implementation handbook for enterprises," 2010.

[25] S. Fraunhofer, "Cloud-computing-sicherheit," 2010. [Online]. Available: http://www.sit.fraunhofer.de/pressedownloads/artikel/bestellung_ccs.jsp

[26] IEEE Intercloud WG (ICWG) Working Group, Online, 2011. [Online]. Available: http://standards.ieee.org/develop/project/2302.html

[27] B. Rochwerger, D. Breitgand, E. Levy, A. Galis, K. Nagin, I. Llorente, R. Montero, Y. Wolfsthal, E. Elmroth, J. Caceres *et al.*, "The reservoir model and architecture for open federated cloud computing," *IBM Journal of Research and Development*, vol. 53, no. 4, pp. 4–1, 2009.

[28] L. Grebe, "Anforderungsanalyse in der Inter-Cloud," master thesis, 2011, Universität der Bundeswehr München.

[29] Amazon, "Amazon web services: Overview of security processes," Online-Quelle, 2011, white Paper. [Online]. Available: http://aws.amazon.com/de/security/

[30] ——, "Amazon web services: Risk and compliance," Online-Quelle, 2011, white Paper. [Online]. Available: http://aws.amazon.com/de/security/

[31] SNIA, "Cloud data management interface (cdmi) v1.0," 2010. [Online]. Available: http://www.developersolutions.org/

[32] PingIdentity, "Pingfederate," 2010. [Online]. Available: http://www.pingidentity.com/

[33] Amazon, "Amazon web services," Online-Quelle, 2011, white Paper. [Online]. Available: http://aws.amazon.com/about-aws/

[34] *Blob Service API (Windows Azure Storage Services REST API Reference)*, Microsoft, 2010. [Online]. Available: http://msdn.microsoft.com/en-us/library/dd135733.aspx

[35] D. K. Taft, "Google, vmware push spring for java cloud development," Online-Quelle, Oktober 2010. [Online]. Available: http://www.eweek.com/c/a/Application-Development/Google-VMware-Push-Spring-for-Java-Cloud-Development-407843/

[36] D. Ogrizovic, B. Svilicic, and E. Tijan, "Open source science clouds," *MIPRO, 2010 Proceedings of the 33rd International Convention*, pp. 1189 – 1192, 2010. [Online]. Available: http://ieeexplore.ieee.org/

[37] OGF, "Open cloud computing interface specification," Online-Quelle, 2010, oGF Open Cloud Computing Interface Working Group. [Online]. Available: http://forge.ogf.org/sf/docman/do/listDocuments/projects.occi-wg/docman.root.drafts.occi_specification

[38] "Deltacloud - many clouds. one api. no problem." Online-Quelle. [Online]. Available: http://deltacloud.org/index.html

[39] "jclouds - project hosting on google code," Online-Quelle, 2010. [Online]. Available: https://code.google.com/p/jclouds/

[40] A. Schellong, "Csc trusted cloud services for defense," Workshop, 2010, presentation at EDA Cloud Computing Workshop.

[41] "Ibm tivoli identity manager: Tivoli.software," Online-Quelle, 2011. [Online]. Available: http://www-142.ibm.com/software/products/de/de/identity-mgr

[42] "Cloud computing management platform by rightscale," Online-Quelle, 2011. [Online]. Available: http://www.rightscale.com/