Towards a Security Management Reference Model for Vertical and Horizontal Collaborative Clouds

Michael Kretzschmar and Sebastian Hanigk
Universität der Bundeswehr München, Institut für Technische Informatik,
Werner-Heisenberg-Weg 39, 85577 Neubiberg, Germany
{michael.kretzschmar, sebastian.hanigk}@unibw.de.

***Abstract*—The re-perimeterization and the erosion of trust boundaries already happening in organizations is amplified and accelerated by Cloud Computing. Security controls in Cloud Computing are, for the most part, no different from security controls in any IT environment from a functional perspective. However, because of the Cloud service models employed, the operational models, and the technologies used to enable Cloud services, Cloud Computing may present different risks and additional requirements to an organization than traditional IT solutions. This paper focuses on security management issues for vertical and horizontal Collaborative Clouds. Based on a detailed and comprehensive analysis of requirement domains, currently offered solutions, security management objects that have to be managed, integrated or adopted, we introduce a Cloud Security Management Reference Model (CSMRM), integrating various Cloud security services of an organization and providing interoperability to identified stakeholders. This new model adopts the Security Management Infrastructure (SMI) approach and establishes the basis for a global and consistent management of the Cloud security infrastructure according to organizational goals.**

***Keywords*-Security Management Infrastructure, Collaborative Clouds, Cloud Security Management Reference Model**

I. INTRODUCTION

Today, every new trend in the Information Technology (IT) has to face issues about security. Most current Cloud offerings are all over the map on the security issue, ranging from largely insecure installations for some commodity and private Cloud offerings to about half of the way towards meeting that goal for the best enterprise public Clouds [1]. One of the most important security challenges is to assure a predefined security level of trust over multi-provider Cloud Computing environments with dedicated communication infrastructures, security mechanisms, processes and policies [2]. Thus, it is necessary to overcome 'security islands' and vendor lock-in. Inadequate security management (in order to establish trust and prevent risks) can be the show stopper for ubiquitous Cloud Computing usage, as Cloud Computing services will multiply and expand faster than the ability of Cloud Computing consumers to manage or govern their usage [3]. Ubiquitous connectivity, the amorphous nature of information interchange, and the ineffectiveness of traditional static security controls which cannot deal with the dynamic nature of Cloud services require enhanced security approaches with regard to Cloud Computing [2], [4].

The aim of Security controls in Cloud Computing is, for the most part, no different than security controls in any IT environment from a functional security management perspective. The Security Management Infrastructure (SMI) approach of the EU [5], NATO [6], the USA [7], or the UK [8], includes security management capabilities such as Identity Management, Privilege Management, Metadata Management, Policy Management, and Crypto Key Management. These functional capabilities will be adopted for Cloud Computing usage [9]. However, the private and public sector needs an objective about how this new computing paradigm will impact organizations from a security management perspective, how it can be used with existing technologies, and the potential pitfalls of proprietary technologies that can result in a lock-in effect or limited choice. To overcome this situation, we present a Cloud Security Management Reference Model (CSMRM) that allows to manage Cloud security management services and to integrate Cloud Computing security management into the (pre-existing) SMI of the whole organization. This CSMRM addresses further challenges and bridges the gap between current insufficient Cloud security management approaches and future Cloud security management.

This paper is structured as follows: In Section II, we provide a detailed description of a collaborative scenario covering all deployment types and delivery models in order to identify Cloud security management relevant components, requirements, and interfaces. In Section III, we provide the results of the requirements analysis, which guides the evaluation of related work in Section IV and the identification of security management objects in Section V. Finally, we introduce the CSMRM in Section VI. Section VII summarises and concludes this paper.

II. SCENARIO

The communication and information infrastructures of private and public sector organizations that are collaborating according to agreed security policies are shown by a scenario in this section (visualized in Figure 1). This infrastructure is controlled and managed traditionally and

 ISBN: 978-1-61208-106-9

includes various security devices, services, and processes from various manufacturers in order to manage IT security capabilities. The organization constructs an internal Cloud Computing infrastructure upon the existing IT infrastructure using open-source or commodity software that includes the Cloud Security Management Infrastructure (CSMI).

A single Cloud (e.g., *PrC-A2* in Figure 1) comprises Cloud services (of one or all types) and additional control and management elements, such as Service Management, Security Management, Service Catalogue, or Collaboration Service. These Cloud services can be used by individuals (e.g., the members of branch *A2* within organization *A*, members of other organizations or external users), and can be a single service or comprise other Cloud services in order to provide the desired functionality.

Services of the same type (SaaS, PaaS, or IaaS) are referred as *horizontal* Cloud services. In many instances, Cloud computing service provider will provide a value-added service on top of another Cloud provider's service. For example, if a SaaS provider needs flexibility, it may be more cost-efficient to acquire necessary infrastructure from an IaaS provider rather than building it. These more complex and integrated services are termed *vertical* Cloud services.

A private Cloud of an organization *A* may contain several Clouds itself (e.g., the Cloud of a branch). The integrated Clouds of organization *A* can be deployed on different geographic locations and organizational branches, subsidiaries, and units. This Cloud can be seen as a *Collaborative Cloud*, even when it is assumed to be a private Cloud from the perspective of organization *A*. Note that a private Cloud service from organization *A* may consist of several Cloud services from partners or from a public Cloud service provider. For example, a Cloud storage service from the private Cloud (*PrC*) of organization *A* may use another Cloud storage service from *PrC-B*, together with a storage system of Cloud *PuC-I*, a file system, and a tape storage system of Cloud *PuC-II*, in order to provide a new compound Cloud service. A Collaborative Cloud may also offer Cloud services which use several other Cloud services, for example an Information service that interacts with various stakeholders of an inter-organizational project.

Clouds are connected via Intranet (private) or Internet (public) connections. In addition, Cloud service brokers—providers that offer intermediation, monitoring, transformation, portability, etc. between various cloud providers—can be used while building compound services. Managers can make intelligent and flexible decisions about what parts of their application loads runs internally and what parts externally. As a rule of thumb, computation-intensive Cloud services are better provided and used by public Cloud providers, but as dynamic security policies may define other risks for the transferred data, such a Cloud service could be moved and deployed back into the private Cloud.

III. Requirements analysis

This section defines the requirements for a unified and collaborative Cloud security management, based on, but not limited to, the scenario given in the previous section. There are several sources [2], [10]–[12] providing questions with regard to Cloud security management (e.g., 'How do I manage and control my security policies along the whole Cloud Service Life-cycle?'). Based on these questions we discovered and defined four domains for Cloud security management requirements to cluster identified requirements. These domains are (1) Security Management Functions, (2) Collaboration, (3) Integration of Security Management Objects, and (4) General Requirements.

A. Security Management Functions

In a hybrid private and public Cloud scenario there is a significant incremental risk if outsourced services to the public Cloud bypass the technical and administrativ controls. Customers are ultimately responsible for the security and integrity of their own data, even when it is held by a service provider [13]. Due to this complexity and opacity, policy enforcement becomes critical at all possible enforcement points. Since it is difficult to ascertain where data may be directed to it becomes imperative to encrypt all data, whether it is in motion or at rest. The biggest question here is key management (e.g., single key for all users, one key per user, multiple keys per user, etc.) [14]. The trend toward multiple service providers has the potential for creating an identity nightmare unless it is coordinated across all platforms. Each service will need to identify the user and may carry a number of user attributes including preferences and history. Federated identity solutions are necessary for service providers to standardize on mechanisms for sharing authentication, authorization and access (AAA) information with each other.

B. Collaboration

Collaborative Clouds are built upon private and public Clouds of various organizations. The following aspects are presented to highlight the requirement spectrum for security management. We probably won't know exactly where or in which country our information is hosted [13]. In addition, information in the Cloud is typically in a shared environment alongside data from other customers. Therefore inter-security management information exchange is necessary, where Cloud security management applications of two or more organizations share information. The use of standardized and non-proprietary protocols to communicate and exchange information between security capabilities will support this inter-organizational sharing of information to prevent vendor lock-in threat, resulting in problems with data transfer between Cloud vendors [15]. Furthermore distributed time zones have to be considered in order to support adequate

 ISBN: 978-1-61208-106-9

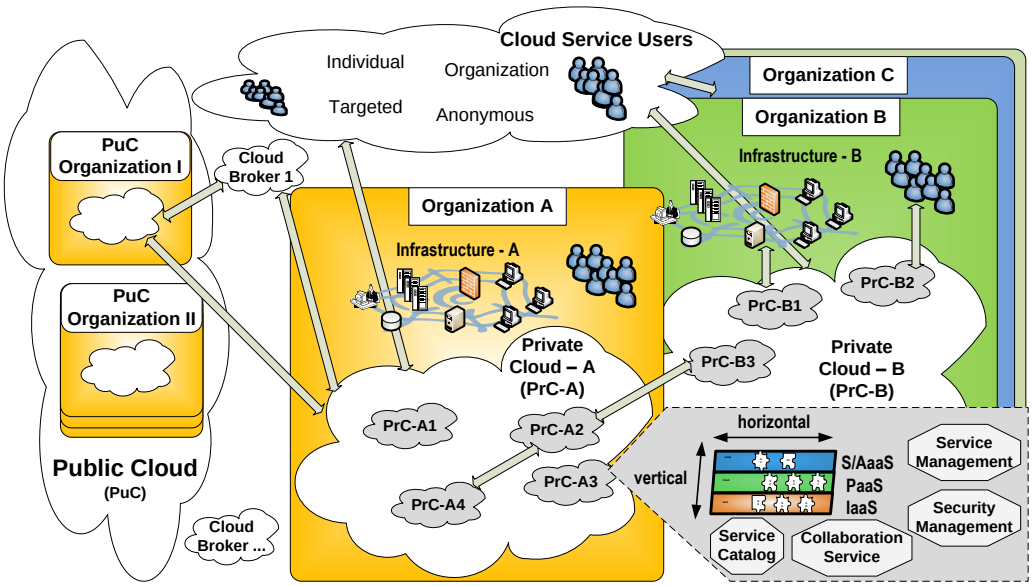

Figure 1. Vertical and Horizontal Collaborative Cloud scenario showing organization-specific private Clouds (*PrC-X*) and public Clouds (*PuC-X*).

timestamps (e.g., security auditing). But also from an intra-organizational perspective security management information exchange between the Cloud security management system and the overarching security management system of the whole organization has to be established in order to fulfill security policies comprehensively.

C. Integration of Security Management Objects

Cloud security management will allow a central operative management of all security capabilities. Therefore it has to provide interfaces and APIs in order to integrate all security-related data stored in the concrete security capabilities including Web-based ones. This will foster the move from manual to automated security management operations. The range of security capabilities that have to be considered by a security management depends mostly on the degree of integration and complexity of the provided services by the Cloud service provider. In the case of SaaS, this means that service levels, security, governance, compliance, and liability expectations of the service and provider are contractually stipulated; managed to; and enforced. In the case of PaaS or IaaS it is the responsibility of the consumer's system administrators to effectively manage the same, with some offset expected by the provider for securing the underlying platform and infrastructure components [2]. However to achieve this integration the adoption of a standards-based system design and implementation to enable interoperability, facilitate federated security management operations is necessary. This allows the use of commercial products, too.

D. General Requirements

As the number of Cloud services and their potential security management capabilities can get quite high in collaborative environments a scalable architecture is required. Additional ones may need to be configured if the collaboration grows or if components are replaced dynamically. But also the set of supported security management capabilities is not static. Continuously, new types of these capabilities evolve and manufacturers are extending their Cloud portfolio. In addition there is the need to operate in a multi-national or multi-cultural environment. Therefore the design and development of the system have to meet the requirements of a specific geographic or linguistic market segment.

IV. Related Work

The following section is structured into two parts. First we provide some theoretical foundations concerning security management models and cloud security areas. Secondly, we present an overview of current Cloud security management approaches and exchange standards.

The FCAPS model (ISO 10164) describes security management functions generically as goals in order to be implemented by security management tools. While the ISO/IEC 27001 offers a methodology and implementation guideline for providing and managing security services. [16] presents a Service Oriented Security Architecture (SOSA) as a collection of security services forming a security infrastructure used by Web Service providers. The Security Management Infrastructure approach, also known as Enterprise Security Management (ESM) will serve as an overarching security architecture integrating security capabilities (e.g., Identity,

 ISBN: 978-1-61208-106-9

Credential, Crypto Key Management, etc.) and managing them according to an organizational security policy [9]. There are several sources that describe Cloud Computing security areas [2], [14], [12], [1]. Unfortunately they differ in defining and covering necessary security management functional areas and collaboration aspects that can be used for a comprehensive Cloud security management. For example the management of meta-data or configuration management of security capabilities are not covered. Mainly they focus only to Identity, Privilege, Access and Crypto Key Management. The adaption and reuse of existing, traditional security management applications for Cloud Computing is proposed as one way-ahead [12]. A detailed summarization of fundamental characteristics and shortcomings of 14 of these security management systems are shown in Figure 2, which compares along a list of 5 design and 9 functional criteria c.q. requirements, indicates that neither of the observed approaches addresses the required range of security management functions, nor do they provide mechanisms for composed Cloud services [17].

Unfortunately only few applications c.q. models that focus unique to the Cloud security management aspect like Zscaler, Panda and the security management model [18] exist. But they only provide single security management function areas like policy-based secure web access or provides complete protection services. Furthermore there are services like PingIdentity, Symplified, etc. that covers the federated management of identities. Mostly there are some security management elements included within Cloud management applications. For example enStratus provides management for Amazon and The Rackspace Cloud infrastructure including security management functions like authentication and authorization, key management and audit. Further examples of Cloud management services like Scalr, Kaavo, CloudKlick, CloudStatus, RightScale, Elastra, Enomaly, Cloud42, etc. exist ([2], [14], [12]). DeltaCloud is an open source project aiming to develop an ecosystem of tools, scripts and applications for the Cloud. The project also aims to write a common, REST-based API to enable developers to write once and manage across multiple Clouds. One of the biggest challenges to Cloud Computing is the lack of standards as many efforts centred around the development of both open and proprietary APIs which seek to enable things such as management, security and interoperability for Cloud. Some of these efforts include the Open Cloud Computing Interface, Amazon EC2 API, VMware's DMTF-submitted vCloud API, Sun's Open Cloud API, Rackspace API, SNIA Cloud Data Management Interface (CDMI) and GoGrid's API, to name just a few. Beside these solutions, there are some standards and approaches for specific security areas. For the exchange of authentication and authorization data, standards as OASIS SAML, specifications of Liberty Alliance, and the Web Services Federation Language are implemented with their main focus on Web-based services. Furthermore in the security area of crypto key management the Key Management Interoperability Protocol (KMIP) can be used.

To summarize current Cloud security management approaches cannot fulfill all requirements put forward for an security management of Collaborative Clouds. The range of security fields supported is often limited and none of these tools are flexible and holistic enough to ensure the required level of interoperability and flexibility by implementing the presented Cloud standards.

V. Cloud Security Management Objects

There are significant trade-offs to each Cloud model in terms of integrated features, complexity vs. openness (extensibility), and security. The key takeaway for security management is that the lower down the stack the Cloud service provider stops, the more security capabilities and management consumers are responsible for implementing and managing themselves. However, there is still the question, what are the 'target objects' that have to be managed within the CSMI. In this section three domains for these objects are introduced that have to be addressed by a Cloud security management system.

A. Security functions provided by Cloud service providers

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) Security supported a multi-factor authentication (knowledge and ownership) to gain access, control privileges and supporting of credentials like X.509 Certificate or proprietary Amazon Secret Access Key (e.g., to sign API calls). A key management allows the multiple concurrent usage of these certificates and keys. Beside that the access is logged and audited. Furthermore flexibility to place instances within multiple geographic regions as well as across multiple availability zones is possible, however the choice (e.g., region, continent) is limited [19].

B. Cloud security management services

PingFederate is a Cloud-based Identity-as-a-Service provider that focus in federating identity management and is integrated by a provider specific API. These kind of Cloud services can be classified as SaaS. The IdP (Identity Provider) sending identity attributes (from an authentication service or application) to PingFederate. PingFederate uses those identity attributes to generate a SAML assertion. PingFederate extracts the identity attributes from the incoming SAML assertion and sends them to the target application of a service provider as consumer of identity attributes. Initial user authentication is normally handled outside of the PingFederate. PingFederate offers integration kits (Windows IWA/NTLM, X.509 Certificate, LDAP Authentication Service), that access

 ISBN: 978-1-61208-106-9

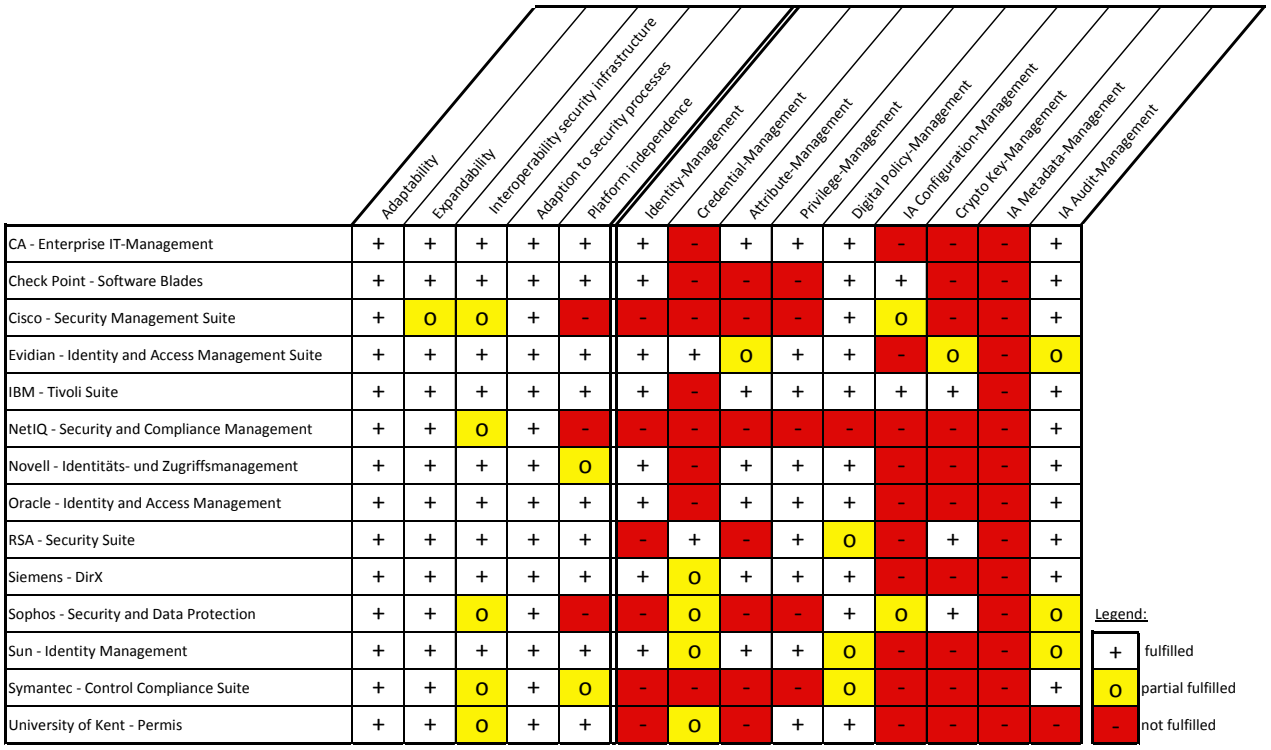

Figure 2. Analysis of current security management approaches

authentication credentials. The IdM agent API (if available) provides the access identity attributes or provided integration kits for CA SiteMinder, Oracle Access Manager (COREid) and Tivoli Access Manager. PingFederate allows a service provider enterprise to accept SAML assertions and provide single-sign-on to applications for Citrix, SharePoint and Salesforce.com [14], [20].

C. Security management objects within interfaces

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 and access controls, data integrity, data at-rest encryption, crypto key management, audit and meta-data management [21]. Some of these security management attributes are *cdmi_security_audit* (If present and 'true', the cloud storage system supports audit logging), *cdmi_security_data_integrity* (If present and 'true', the cloud storage system supports data integrity/authenticity) or *cdmi_security_encryption* (If present and 'true', the cloud storage system supports data at-rest Encryption).

VI. Cloud Security Management Reference Model

In this section an reference model for Cloud security management is presented based on the detailed requirement analysis and the Cloud security managed objects. The CSMRM, which is shown in Figure 3, will serve as a comprehensive guideline in order to implement and design Cloud security management systems that address the highlighted security spectrum.

Within the requirement analysis we identified four domains in order to cover the range of requirements and functions for security management. Consequently the CSMRM consists of four interoperating layers - *Adapter and Libraries Layer, Platform Service Layer, Functional Service Layer, and Collaboration Service Layer*. The CSMRM adopts a standards-based system design and implementation that enable interoperability, facilitate federated security management operations, allow the use of commercial products and ease evolution. Therefore, it includes 5 domains of interfaces and APIs for the Collaborative Cloud environment. Here a Cloud security management system has to interact with (1) the Security Management Infrastructure of the organization, (2) the security managed objects, (3) other Cloud security

 ISBN: 978-1-61208-106-9

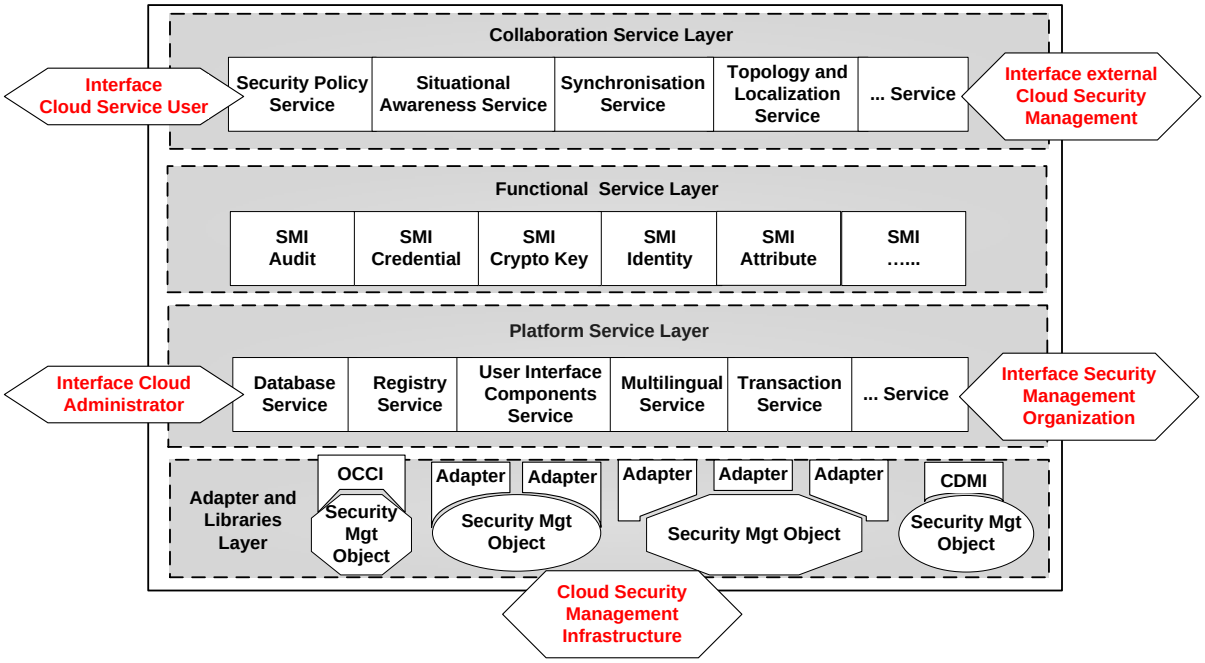

Figure 3. Cloud Security Management Reference Model

management systems (e.g., Cloud Broker, partners, public Cloud providers), (4) Cloud Service User, and (5) Cloud security roles within the organization (e.g., administrator, security officer, etc.). The lowest layer is called *Adapter and Libraries Layer*, which integrates and accesses various Cloud security management objects. These objects differ in two dimensions: First, how a the object is interfaced with. Each one may have its own protocol for communication (e.g., LDAP, proprietary APIs, or Simple Object Access Protocol (SOAP) in case of a Web Service). Second, the function a concrete object provides. The requirement to map all these different protocols and function sets to a Cloud security management system bears therefore a high degree of complexity. The proposed solution is abstraction and service decomposition, as the *Adapter and Libraries Layer* consists of different types of adapters and libraries, where each type may have a number of security management object-dependent implementations. Each adapter has two interfaces: a primitive function interface, which is common for all adapters of one type, and a object-dependent interface, which implements the (proprietary) interface of the concrete security managed objects. If available the adapter type will be defined and implemented according to standards like SAML, KMIP, OCCI, or CDMI. Above that the *Platform Service Layer* provides basic services to the Cloud security management system and implements the integration within the SMI of the organization. For example a *Database Service* including backup functionality will serve as the underlying security management data storage for the future system. For specific purposes different database types like structured and unstructured ones are offered. A *Registry Service* is necessary in order to have an overview about all system components within the Cloud security management system. Further a *Multi-lingual Service* allows a user to define, select, and change between different culturally-related application environments to support the usage within Collaborative Clouds. The *Functional Service Layer* includes all security management functional areas like Identity Management, Privilege Management, Metadata Management, Policy Management and Crypto Key Management. These services comprise all elements of their area within one organization. A *Collaboration Service Layer* is at the top of the CSMRM that support the inter-security management information, where Cloud security management applications of two or more organizations share information in Collaborative Clouds. The use of standardized and non-proprietary protocols to communicate and exchange information between security capabilities will support this inter-organizational sharing of information to prevent vendor lock-in threat. A *Security Policy Service* guarantees that regulations and constrains of the organization are enforced even when the combined Cloud service respective security data is distributed and located at various geographic units within the collaboration. In addition a *Topology and Localisation Service* provides an up-to-date view of the orchestrated collaborative environment, that supports other services of that layer. Underlying to these is a *Synchronization Service* that allow the exchange and transaction between various technologies and timezones.

 ISBN: 978-1-61208-106-9

VII. CONCLUSION

Identifying and defining security management issues for Cloud Computing are challenging tasks. Though inadequate security management in order to establish trust and preventing risks can be the show stopper for ubiquitous Cloud usage as Cloud services will multiply and expand faster than the ability of Cloud consumers to manage or govern them in use. Ubiquitous connectivity, the amorphous nature of information interchange, and the ineffectiveness of traditional static security controls which cannot deal with the dynamic nature of Cloud services, all require new security thinking with regard to Cloud Computing in the context of Collaborative Clouds. However an objective about how this new computing paradigm will impact organizations from a security management perspective, or how it can be used with existing technologies, and the potential pitfalls of proprietary technologies that can lead to lock-in and limited choice, is needed. To overcome this situation we presented a Cloud Security Management Reference Model that enables potential users to manage various horizontal and vertical Cloud security services independent of their complexity. The adapter and library layer allows the integration and clustering according SMI functions that guarantees a comprehensive coverage of all security management aspects. Furthermore it support the collaboration with Cloud service users and other Clouds. Due to the fact that such a comprehensive Cloud security management model does not exists yet, it will serve as a guideline to design and implement future Cloud security management systems.

ACKNOWLEDGEMENT

The authors wish to thank the members of the Chair for Communication Systems and Internet Services at the Universität der Bundeswehr Munich, headed by Prof. Dr. Gabi Dreo Rodosek, for helpful discussions and valuable comments on previous versions of this paper. The Chair is part of the Munich Network Management Team. Furthermore, we would like to acknowledge the support and contribution of the NATO SC/4 SMI AHWG and the European Defence Agency's PT CIS. This research activity has been performed partially in cooperation with the Federal Office for Information Security.

REFERENCES

[1] THE 451 GROUP, *CLOUDSCAPE - Cloud Codex*, www.451group.com/reports/executive_summary.php?id=869, last access: 23-08-20010

[2] Cloud Security Alliance, *Security Guidance for Critical Areas of Focus in Cloud Computing V2.1*, 2009

[3] R. Miller, *Cloud Brokers: The Next Big Opportunity?*, Data Center Knowledge, http://www.datacenterknowledge.com/archives/2009/07/27/cloud-brokers-the-next-big-opportunity/, last access: 23-08-20010

[4] A.V. Dastjerdi, K.A. Bakar, and S.G.H. Tabatabaei, *Distributed Intrusion Detection in Clouds Using Mobile Agents*, Advanced Engineering Computing and Applications in Sciences, 2009. ADVCOMP '09. Third International Conference on , pp.175-180, 2009

[5] EDA, *End-to-End Security Management in a Heterogeneous Environment*, EDA 08-CAP-027, 2009

[6] NATO, *Concept of a NATO Security Management Infrastructure*, AC/322(SC/4-AHWG/3)WP(2007)0001), 2008

[7] NSA, *Enterprise Security Management: A context overview*, 2009

[8] CESG, *Study on Security Management Infrastructure*, http://www.cesg.gov.uk/, last access: 23-08-20010

[9] M. Kretzschmar and F. Eyermann, *A Multi-Layer Architecture for a Security Management Infrastructure* , MilCIS 2009 Conference Paper, 2009

[10] Jericho Forum, *Cloud Cube Model v1.0: Selecting Cloud Formations for Secure Collaboration*, 2009

[11] DMTF - Open Cloud Standards Incubator, *Interoperable Clouds-A White Paper from the Open Cloud Standards Incubator*, 2009

[12] SIT Fraunhofer, *Cloud-Computing-Sicherheit*, http://www.sit.fraunhofer.de/pressedownloads/artikel/bestellung_ccs.jsp, last access: 23-08-20010

[13] B. Kandukuri, V. Paturi, and A. Rakshit, *Cloud Security Issues*, Services Computing Conference 2009 - SCC '09, pp. 517 - 520, 2009

[14] J. Rhoton, *Cloud Computing Explained: Implementation Handbook for Enterprises*, Recursive Press, 2010

[15] T. W. Wlodarczyk, C. Rong, and K. A. Haaland Thorsen,*Industrial Cloud: Toward Inter-enterprise Integration*, Cloud Computing, 2009

[16] C. Opincaru, *Service Oriented Security architecture applied to Spatial Data Infrastructures*, Universität der Bundeswehr München, Dissertation, 2008

[17] M. Knüpfer, *Analyse und Bewertung von SMI Anwendungen*, Bachelor thesis (in German), Information System Laboratory, University of the Federal Armed Forces Munich, Germany, 2010

[18] Y. Jung and M. Chung, *Adaptive security management model in the cloud computing environment*, Advanced Communication Technology (ICACT) 2010, vol. 2 pp. 1664 - 1669, 2010

[19] Amazon, *Amazon Web Services: Overview of Security Processes*, http://aws.amazon.com/de/security/, last access: 23-08-20010

[20] PingIdentity, *PingFederate*, http://www.pingidentity.com, last access: 23-08-20010

[21] SNIA, *Cloud Data Management Interface (CDMI) v1.0*, http://www.developersolutions.org/, last access: 23-08-20010

 ISBN: 978-1-61208-106-9