MuSIC: An IT Security Architecture for Inter-Community Clouds

Gabi Dreo Rodosek
Universität der Bundeswehr München
MNM-Team
Neubiberg, Germany
Email: gabi.dreo@unibw.de

Mario Golling
Universität der Bundeswehr München
MNM-Team
Neubiberg, Germany
Email: mario.golling@unibw.de

Wolfgang Hommel
Leibniz Supercomputing Centre
MNM-Team
Garching, Germany
Email: wolfgang.hommel@lrz.de

***Abstract*—The evolution towards the Inter-Cloud (a global "cloud of clouds") represents a huge developmental leap for cloud computing, enabling new innovative value-added services. Naturally, one of the main issues of interconnecting clouds is security (i. e., Inter- or Intra-cloud security). *MuSIC* addresses this issue by proposing an IT security architecture which concepts have been developed on the basis of the input of more than 25 leading research and industry organizations from the Munich Security Cluster. Based on requirements derived from realistic and innovative Inter-Cloud use cases, the architecture with six core modules has been defined and corresponding IT Service Management processes have been specified.**

I. Introduction

Despite the economic attractiveness and the undisputed market potential, the use of cloud computing by enterprises outside the USA is still relatively low. With the high numbers of security-related incidents throughout the last years, the public as well as the industry have been made aware of difficulties of IT security in general and thus also for the secure usage of cloud computing. In this context, the security of enterprise data is one of the mandatory topics. In addition, data protection laws, especially within Europe, are also obstacles for the use of today's cloud computing solutions.

Thus, the *MuSIC (Munich Secure Inter-Community Cloud)* IT security architecture has been developed in close cooperation with several partners from industry (including BMW Group, Allianz, Telefonica, and Bosch Security Systems) with the purpose of (i) providing a solution for the conflicting requirements between the secure use of cloud computing and the realization of the economic benefits, and (ii) using the Inter-Cloud for the development of innovative services.

This paper gives an overview of *MuSIC*'s core modules and IT service management processes, and is organized as follows: Section II gives an overview of an use case for Inter-Clouds and its requirements. Section III reviews related work. In Section IV, the *MuSIC* IT security architecture is presented. A short summary and outlook conclude the paper.

II. Inter-Cloud Scenario and Requirements

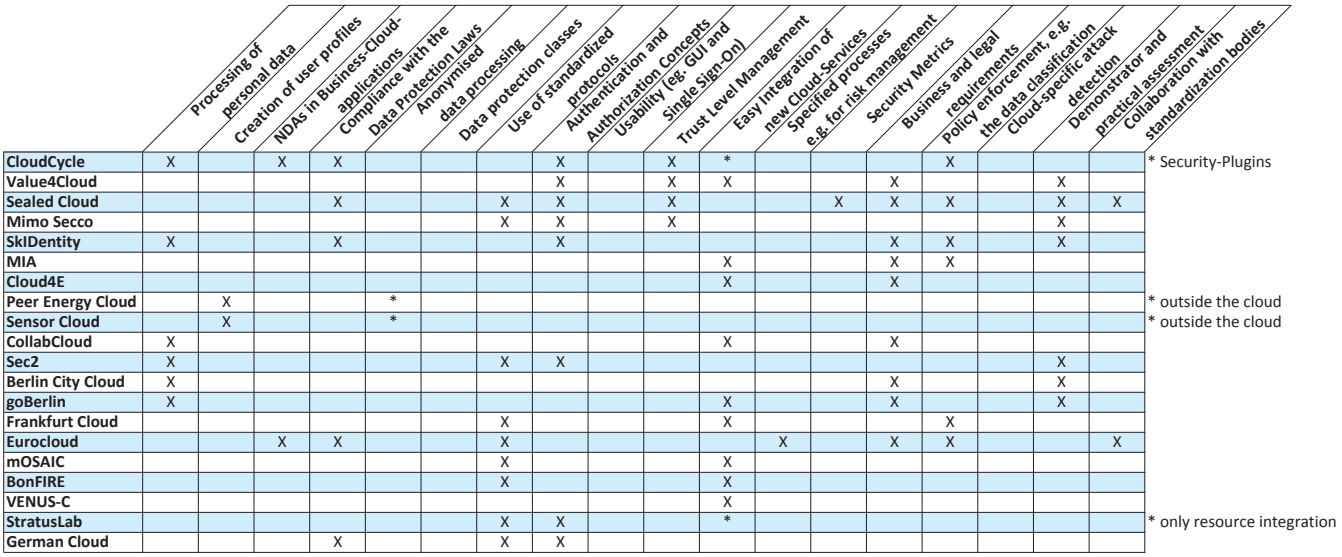
A. Scenario: Inter-Cloud-based Navigation

Satellite navigation systems are used widely because of their ability to evaluate maps, including properties of roads and selecting the most appropriate route (e. g., prefer highways). With the use of the so-called Traffic Message Channel (TMC), the underlying information can be enriched with recent developments, e. g., accidents. However, this technology is limited in scope. Combining data from different sources (e. g., intelligent traffic management, accident blackspots, and roadblocks), provided by different organizations or community clouds, allows (i) to calculate even better routes, and to (ii) optimize the traffic flows globally by preventing and mitigating traffic jams, cleaning routes for emergency vehicles, and reducing the overall risk of accidents. The main challenge in correlating different data from different sources is the concern of the "data providers" about access and usage. The worry of loosing control is one of the main obstacles of organizations for not participating in Inter-Clouds.

B. Requirements Analysis

Based on this and other scenarios, requirements were derived in *MuSIC*. One major requirement refers to the *control of data* (e. g., who is accessing data). Furthermore, *regulations regarding privacy* do have a strong impact. Methods need to be developed that process data as far as possible in an anonymous way. Moreover, *data security* has to be guaranteed especially when sensitive data is stored in the Inter-Cloud. The technical implementation has to include secure data storage and data processing as well as secure transport of data. It is necessary to specify different *data protection classes*. Existing protocols in the field of cloud computing can serve as a basis, but need to be extended for the assignment of data to certain data protection classes. The composition of individual clouds requires mutual, *verifiable trust* among partners and therefore a trust management system. On the basis of determined, objective measures, a classification of participating providers must be made. The secure, multi-agency approach for exchanging and sharing data requires a cross-organizational authentication and authorization infrastructure (AAI). Thus, an *federated identity management (FIM)* for Inter-Cloud environments is essential. Inter-Clouds produce *new attack vectors and possibilities for abuse*, which have to be identified more accurately. Attack detection from a cloud or in a cloud in an Inter-Cloud environment requires the development of cross-organizational (cross-cloud) Intrusion Detection Systems (IDS). Besides, the so-called vendor lock-in effect needs to be addressed by standardized APIs and compatible software.

978-3-901882-50-0



	Processing of personal data	Creation of user profiles	NDAs in Business-Cloud-applications	Compliance with the Data Protection Laws	Anonymised data processing	Data protection classes	Use of standardized protocols	Authentication and Authorization Concepts	Usability (eg. GUI and Single Sign-On)	Trust Level Management	Easy Integration of new Cloud-Services	Specified processes e.g. for risk management	Security Metrics	Business and legal requirements	Policy enforcement, e.g. the data classification	Cloud-specific attack detection	Demonstrator and practical assessment	Collaboration with standardization bodies	
CloudCycle	X		X	X			X		X	*			X						* Security-Plugins
Value4Cloud							X		X	X			X				X		
Sealed Cloud				X			X	X		X		X	X	X			X	X	
Mimo Secco							X	X		X							X		
SkIDentity	X			X				X					X	X			X		
MIA										X			X	X					
Cloud4E										X			X						
Peer Energy Cloud		X			*														* outside the cloud
Sensor Cloud		X			*														* outside the cloud
CollabCloud	X									X			X						
Sec2	X						X	X									X		
Berlin City Cloud	X												X				X		
goBerlin	X									X			X				X		
Frankfurt Cloud							X			X				X					
Eurocloud			X	X			X				X		X	X				X	
mOSAIC							X			X									
BonFIRE							X			X									
VENUS-C										X									
StratusLab							X	X		*									* only resource integration
German Cloud				X			X	X											

Fig. 1. Comparison of some current cloud projects with regard to IT security aspects

III. Related Work

Cloud computing is currently being investigated by many industrial organizations, scientific researchers, studies, and projects from several angles. Among the best known European studies on cloud computing is the study of ENISA [1], focusing primarily on the perspective of cloud computing users. Complementary to this, the BSI highlights the minimum security requirements for cloud computing services. Even the U.S. NIST aims to develop new industry standards and solutions, including interoperability, portability, and security. Furthermore, also the Cloud Security Alliance defines the security principles for cloud providers in order to improve the assessment of security risks. For this purpose, the Alliance provides a framework for a detailed understanding of security concepts and principles for cloud security standards. The Global Inter-Cloud Technology Forum (GICTF) promotes world-wide standardization of Inter-Cloud system interfaces to ensure interoperability; the focus is the guaranteed availability of services from partial system failure within Inter-Clouds. Several Inter-Cloud security-related issues are already investigated extensively in other publications, such as secure data transfer and secure data backup. Several research projects, for instance, deal with the security of the virtualization techniques.Furthermore, the Trusted Cloud initiative of the Cloud Security Alliance OASIS and the Open Identity Exchange Initiative focus on the secure identity and access management in the context of cloud computing. In this context, the scientific work of Bertino et al. [2] pays special attention to the protection of personal data of users of cloud services.

Quite a large number of projects discuss cloud computing with a focus on security. In the following, due to brevity reasons, only a few selected projects can be discussed as summarized in Figure 1. We focus on projects that deal with several aspects of cloud security in parallel. In addition, there are other projects, which deal with selected basic technologies, such as Identity Management in the cloud environment. Here, data protection aspects are considered, i. e., whether personal data is processed, conscious user profiles are created, non-disclosure agreements are provided in the context of industrial applications or the conformity is explicitly addressed by the data protection laws and how an anonymized data processing is provided. It is also considered whether the use of standardized protocols is possible and whether explicit concepts for authentication, authorization, and trust management levels exist. Apart from the simple extensibility with new services and the consideration of business and legal requirements, also the practical implementation, e. g., in the form of a demonstrator, was investigated.

In a nutshell, especially aspects such as *(i)* the definition of data protection classes, *(ii)* user-friendly security mechanisms, e. g., single sign-on, *(iii)* explicit cloud-risk management, *(iv)* the use of quantifying security metrics (i. e., metrics that can be measured and calculated), and *(v)* cooperation with standards bodies needs to be strengthened. In addition, also the Inter-Cloud needs to be addressed more deeply.

IV. IT Security Architecture for Inter-Community Clouds

Security, trust, and privacy are fundamental for the further development of Inter-Clouds. *MuSIC* provides an essential contribution by providing solutions for associated security aspects of community clouds. A community clouds is a shared cloud infrastructure between several organizations of a specific community with common concerns. Beside the sharing of resources in terms of IaaS (Infrastructure as a Service), Inter-Community Clouds and the Inter-Cloud allow to aggregate data from their member organizations in order to build value-added cloud services. Such services typically have proprietary interfaces, i. e., dedicated *apps* are required to access and use them. Therefore, one of *MuSIC*'s goal is to provide a stable subset of *core modules* for any type of Inter-Community Cloud, based upon additional, application-specific modules can be developed.

Given the related work and existing Inter-Community Cloud approaches, internally the Inter-Community Clouds rely on concepts that are very similar to those that have been applied under the term *federation* for inter-organizational collaboration efforts. Therefore, for the design of *MuSIC* we were able to leverage several concepts for so-called circles-of-trust, a term coined by the former Liberty Alliance, which is meanwhile known as the Kantara Initiative [3].

The most valuable asset within an Inter-Community Cloud, and also other clouds, is *data*. The ultimate goal of any Security Architecture therefore is to provide adequate security measures to protect this data, e. g., from disclosure, unwarranted modifications, or attacks against its availability.

A. Data Protection Classes, Cloud Tagging

Storing and processing data in clouds is one of the essential aspects. Quite often, data is stored encrypted with the limitation that no data processing is possible in the cloud. Solutions like homomorphic encryption (e.g., [4]), a process by which calculations can be performed on encrypted data, are still undergoing research. The assumption under which concepts for data protection need to be developed is that the cloud environment (except private clouds) is insecure, and that data itself needs to be protected. Thus, we need to consider *data as managed objects.*

Inter-Community Clouds are built upon service level agreements (SLAs). In order to specify what may and must not be done with any specific managed object, e. g., by means of access policies, data first needs to be classified. *MuSIC* uses a cloud data protection model that includes for example the following attributes: (i) object identifier, (ii) owner of the data, (iii) criticality of the data from the enterprise's viewpoint, (iv) classified level. Access control lists are applied with groups (including everyone, named groups, or single persons, apps), permissions (either coarse-grained like read or write, or fine-grained, such as search, use, copy, modify, delete, print etc.), and obligations (such as to log the access, send an alert on access etc.). Along with this classification of data, *MuSIC* introduces a *tagging* scheme: (i) clouds are tagged in order to quickly identify whether a cloud is suited to store the various types of data, depending on the security mechanisms that are in place, and (ii) services and *apps* are tagged to determine, which of them accesses data in the Inter-Cloud that has been classified. When applied in a single Inter-Community Cloud, this tagging scheme enables a quick check whether a particular data may be stored in the cloud. Its true strength, however, lies in the ability to determine admissible workflow paths when passed through Inter-Cloud workflows.

B. Core Modules of the Security Architecture

MuSIC's core modules are the following:

- **Identity Management**: This module encompasses the XRI-based identification of users, devices, apps, data, clouds, and further entities. Each type of identity has a specific data model. *MuSIC* also incorporates reliable authentication and role-based authorization concepts. While [5] has suggested new terms and concepts for Inter-Cloud Identity Management, including the definition of so-called home clouds and foreign clouds, *MuSIC* sticks to the more classical approach of having exactly one identity provider per identity. The primary motivation for this design decision is to leverage existing Identity Management infrastructures: Instead of re-enrolling all users in the Inter-Community Cloud and therefore forcing users, e. g., to change their authentication means to a home-cloud-wide uniform method, existing user databases and identity repositories can be integrated as long as common protocols for the exchange of identity and authorization information, such as SAML, are supported.
- **Trust Level Management**: The Trust Level Management module addresses the determination and monitoring of the trust level of each involved cloud. A trust level basically correlates with the data protection classification and can never exceed it. For example, non-personal data may be stored in a cloud that is tagged for handling personal data, but highly critical data must not be stored in a cloud that can handle only lowly critical data. However, trust levels vary based on the formal relationship, which the data owner has with the respective Inter-Community Cloud as well as classic trust factors, such as past experiences and a reputation system. Basic trust values are derived from organizational measures, such as contracts and SLAs. If the cloud, whose trust level is to be estimated, has been involved in previous workflows, classic trust factors are evaluated to dynamically determine the current trust level.
- **Attack Detection**: Just like in enterprise networks, attack detection needs to be performed in Inter-Community Clouds. New attack vectors that cannot be detected by existing enterprise-grade Intrusion Detection Systems (IDS) must be covered. Even though the *MuSIC* architecture creates Inter-Clouds with security in mind from the scratch, the increasing complexity of Inter-Cloud services, the short time-to-market for *apps* and the overall budget pressure lead to the demand for cloud-wide attack detection and quick responses to detected security incidents. *MuSIC*'s approach in this discipline is a thorough registration of legit communication processes along with the definition of measurement points, for example, at Inter-Cloud nexuses. Based on results in Grid IDS [6], an extension of the XML-based IDMEF format is used for the exchange and correlation of security alerts.
- **Discovery of Resources and Services**: *MuSIC* features a decentralized registry for shared resources and services that can be used by the other Inter-Community Cloud members. Each cloud member registers the resources it is willing to share and updates the registration data based on, for example, current workload, scheduled downtimes, and dynamic billing information.
- **Data Vault**: In practice, each Inter-Community Cloud will have an acceptable trust level for each of its members, and Inter-Cloud workflows can only be established if each involved cloud and the data that has to be processed share the same tags. Therefore, most use cases for Inter-Cloud will not require data

encryption except when data has to be stored at an untrusted organization that is not otherwise involved in processing of the data. For this particular case, and because there is currently a practical demand for such a service due to most organizations' perception of cloud services as of today, *MuSIC* provides a *data vault*, i. e., an encrypted data storage area with an explicit data access service that is operated by one of the members of the confidential workflow.

- **Security Metrics**: Measuring and reporting security properties of the Inter-Community Cloud is a key feature to ensure high acceptance.The *MuSIC* security architecture defines measurement points and procedures, supports the automated generation of security reports for various target audiences, and ensures that derived results are incorporated into the planning of service enhancements as part of the continuous improvement process. Security metrics can also be evaluated during the calculation of trust levels, so that failing short of target values may result in a degradation of the trust level.

C. IT Service Management Processes

The involvement of multiple service providers and the complex inter-organizational workflows necessitate a solid IT Service Management (ITSM). As a consequence, also the Inter-Cloud adaptation of ITSM processes is a part of the *MuSIC* project. ITSM best practices, e. g., ITIL v3, and ITSM standards, such as ISO/IEC 20000, have been designed with an explicit focus on single organizations. Therefore, even organizations that already have established formal management processes face new challenges when participating in Inter-Community Cloud and Inter-Cloud services.

So far, only few reference management processes have been specified for inter-organizational settings: For example, Marcu deals with inter-organizational fault management in [7]. In *MuSIC*, we focused on the following selected IT service management processes.

1) ***Incident Management****:* Incident management basically includes the handling of any deviation from a service's nominal condition. For each Inter-Community Cloud, *MuSIC* proposes the operation of a central service desk, which on the one hand serves as a contact for manually detected or assumed incidents and on the other hand is responsible for the coordination of repair measures.

2) ***Configuration Management****:* Several workflows in *MuSIC* are built upon the concept of an Inter-Community Cloud configuration management database (iccCMDB), which extends ITIL's key component for managing assets. Besides an inventory of the resources that have been made available to the Inter-Community Cloud by its members and the services that are realized based on them, the iccCMDB supports other processes by, e. g., providing information about contacts and dependencies from other so-called configuration items.

3) ***Capacity Management****:* Organizations join Inter-Community Clouds primarily either to draw profit by sharing resources which they cannot fully utilize all the time or because they have temporary demands for additional resources that would be uneconomic to set up in-house. Other than the key capacity issues for cloud service providers that deal with a basic supply/demand balance, capacity management for Inter-Community Clouds needs to be based on more foresighted strategies in order to avoid skews and overprovisioning.

4) ***Change Management****:* Changes to resources and services need to be coordinated in an Inter-Community Cloud-wide manner to avoid service incidents. This includes the reconfiguration of software, scheduled maintenance tasks, the addition of new resources to the cloud, and the deprovisioning of resources and services. All these changes need to be planned, submitted for approval, communicated in due time, documented, and coordinated while they are implemented.

V. Conclusions and Outlook

Inter-Clouds that allow the interaction between "isolated" cloud systems are the next step towards an even more efficient resource sharing, aggregation and correlation of data, and the development of novel cloud-based apps. Assuring security, privacy, and trust are, however, preconditions. Based on innovative and realistic scenarios, *MuSIC* addresses proposes a security architecture for Inter-Community Clouds as well as the necessary IT service management processes. The developed demonstrator shows the applicability of the developed concepts. Having the architecture defined, a further refinement of the core modules, the development of innovative cloud-based apps, an update of the demonstrator as well as the development towards common technical standards are the next steps.

Acknowledgment

The authors wish to thank the Munich Network Management Team (LMU, LRZ, UniBwM), Fraunhofer AISEC as well as employees of Allianz, BMW, Bosch, FUJITSU, Giesecke & Devrient, Infineon, Telefonica, the City of Munich and various other companies for their valuable advices and discussions.

References

[1] D. Catteddu and G. Hogben, Eds., *Cloud Computing – Benefits, risks and recommendations for information security*. The European Network and Information Security Agency (ENISA), 2009.

[2] E. Bertino, F. Paci, R. Ferrini, and N. Shang, "Privacy preserving digital identity management for Cloud-Computing," *IEEE Data Eng. Bull.*, vol. 32(1), pp. 21–27, 2009.

[3] R. Hörbe, "Trust Framework Meta Model - Kantara Initiative," 2011. [Online]. Available: http://kantarainitiative.org/confluence/display/TFMMWG/Home

[4] C. Gentry, "A fully homomorphic encryption scheme," Ph.D. dissertation, Stanford University, 2009, crypto.stanford.edu/craig.

[5] A. Celesti, F. Tusa, M. Villari, and A. Puliafito, "Security and cloud computing: Intercloud identity management infrastructure." in *Proc. WETICE 2010*, S. Reddy, Ed. IEEE Computer Society, 2010, pp. 263–265. [Online]. Available: http://dblp.uni-trier.de/db/conf/wetice/wetice2010.html#CelestiTVP10

[6] N. gentschen Felde, W. Hommel, J. Kohlrausch, H. Reiser, C. Szongott, and F. von Eye, "A Grid-based Intrusion Detection System (GIDS)," in *Book of abstracts – a 360° perspective on IT/IS in higher education*, ser. EUNIS 2012 – 18th EUNIS Congress, B. Fonseca, Ed. Vila Real: Universidade de Trás-os-Montes e Alto Douro, Jun. 2012, pp. 185–186.

[7] P. Marcu and W. Hommel, "Interorganizational fault management: Functional and organizational core aspects of management architectures," *International Journal of Computer Networks & Communications (IJCNC)*, vol. 3, no. 1, pp. 101–117, 2011.