International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 10 Issue 5 ǁ 2022 ǁ PP. 04-06

Security Management realm within theInter-Cloud

Annesh P, PG Scholar
Department of MCA, Dayananda Sagar College of Engineering,
Bengaluru, Affiliated to VTU

Abstract—*Within the context of Cloud Computing, one of the most important security challenges is to manage and assure a secure usage over multi-provider Inter-Cloud environments with dedicated communication infrastructures, security mech- anisms, processes and policies. 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 adaption and reuse of existing traditional security management areas that have to be enhanced for specific Cloud computing requirements (e.g., dynamic reconfiguration, distributed services, etc.), is proposed. Based on the collection of various Inter-Cloud use cases and scenarios within the private and public sector like DMTF (Distributed Management Task Force), NIST (National Institute of Standards and Technology), GICTF (Global Inter- Cloud Technology Forum) and ENISA (European Network and Information Security Agency) we analyzed and summarized the range of requirements for security management. As these requirements are not yet fulfilled by current security manage- ment approaches, we derived a set of security management areas that describe all identified functional aspects. This set will serve as a foundation of our future development towardsa security management architecture for the Inter-Cloud.*

Keywords-*Security Management Infrastructure, Cloud Secur- ity Management, Inter-Cloud, Cloud Computing*

Date of Submission: 08-05-2022 Date of acceptance: 23-05-2022

I. PROBLEM DESCRIPTION

The Inter-Cloud as 'an interworking of Cloud systems of different Cloud providers' accelerates the erosion of trust boundaries already happening in organizations [1]. In the Inter-Cloud environment, overall security issues and require- ments can be evaluated from the points of Cloud providers and customer. In addition, a provider that participates in both roles 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.

However, the implementation of such Inter-Cloud en- vironments is not trivial at all because Clouds are more complicated than traditional systems and the existing interop- erability and orchestration models are not applicable. In fact, while Clouds are typically dynamic, the existing models are designed for static environments where dynamic agreements among the parties are needed to establish a federation [2]. Keeping in mind the aforementioned environment, we present some of the Inter-Cloud management challenges focusing on security management.

Samitha Kahiyum , Head of the Department,Department of MCA,
Dayananda Sagar College of Engineering,Bengaluru, Affiliated to VTU

If a Cloud provider experiences an unexpected overload or a natural disaster, he will require spare Cloud services to cope with the situation. In order to guarantee the required service quality, such as service availability and performance, even in such cases, there will be the need to provide a mechanism for flexibly reassigning Cloud services among Cloud systems. A Cloud provider can on the one hand alter the data for the service connection point accessed by his customers to access another Cloud system, or on the other hand act as a proxy between his customers and the other provider. Therefore the providers exchange customer IDs and other data between the Cloud systems for interaction so that the customers can access services under the same conditions [3]. Especially from a security management perspective there is the need for an integration of different security technologies, permitting a Cloud provider to be able to join the Inter-Cloud without changing his security policies or authorisation processes [2]. For a Cloud customer it is important to select trustworthy Cloud providers and Cloud systems that meet his quality requirements, based on matching the customer's quality requirements with the provider's SLA [3]. Also the Cloud provider itself has to search and discover Cloud services that satisfy the requirements (region,

encryption, etc.) of his customers in his own Cloud system or other Cloud systems. At the moment, a provider does not know which security management functions and information have to be provided in order to exchange such security preferences between Inter-Cloud elements. Due to the dynamics of an Inter- Cloud federated infrastructure, a flexible method for building dynamic interactions and enabling the coexistence of different and heterogeneous technologies should be provided [2]. In addition, well-established security management approaches have to be considered and for instance in the case of the public sector they are sometimes even mandatory.

II. SECURITY MANAGEMENT AREAS FOR CLOUD COMPUTING

In ITILv3 and ISO/IEC 20000, Security Management (SM) includes functions that control and protect access to organiz- ation's resources, information, data, and IT services in order to ensure confidentiality, integrity, and availability. Security management functions are methods for for authentication, authorization, encryption, etc. Unfortunately, the expanded definitions and standards around security management do not define a common set of security management areas. For example, in the FCAPS model (ISO/IEC 10164), security management functions are generally described as goals in order to be implemented by security management tools. On the other hand, ISO/IEC 27001 establishes a code of conduct for Information Security Management, which offers a methodology and implementation guideline for providing and managing security services.

The Security Management Infrastructure approach, which is also called Enterprise Security Management (ESM) is known to serve as a comprehensive security architecture for our research [4]. This approach of EU, NATO, the UK, and the USA [5], [6] contains security management func- tions, such as Identity Management, Privilege Management, Metadata Management, Policy Management, and Crypto Key Management. In addition, there are several sources that describe Cloud computing security areas [7], [8]. However, they differ in their compliance with 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 on Identity, Privilege, Access, and Crypto Key Management.

Based on the presented sources above, we present the fol- lowing ten security management areas for Cloud computing, that can be briefly described as follows:

Identity Management is the ability to confirm and manage the life cycle of an assured identity (human/device/process). Federated Identity Management provides end users with secure access across multiple external applications 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, badges, passwords and keys. The credential management is also responsible for verifying the authenticity of credentials. *Attribute Management* is the ability to manage the assigned properties of entities. An attribute is a specification which defines a property of an object. Furthermore, it is responsible for requesting the new attribute and associated values from service upon attempts to access the service.

Privilege Management is the ability to manage permissionsto perform an action.

Digital Policy Management is the ability to generate, convert, manage and replace digital policies. Digital policies are those that are in machine-specific languages and can be used to guide the behavior of systems in an automated or semi- automated manner.

Configuration Management manages the security-related configuration items, such as defining, controlling, ordering, and loading of configuration data for services.

Cryptographic Key Management encompass all of the activ- ities 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 schema and values over their life-cycle.

Audit Management is the ability that establishes auditable security-relevant events which lead to the monitoring of the behavior services allowing in turn for the analysis and reporting of the current and past situation leading to securitysituational awareness.

SM Information Management is the ability to gather and manage security-relevant information of Cloud services (such as region, time, etc.) that are not a native component of the security management areas.

III. FUTURE WORK

Based upon the presented security management areas, functional and process components for a Security Manager architecture in the Inter-Cloud need to be identified and defined. Together with derived security data artifacts, this will support the Cloud provider community to implement a Security Manager system for a future Inter-Cloud environ- ment and facilitate the adoption of this results in the private and

public sector.

ACKNOWLEDGEMENT

This research activity has been supported partially in cooperation with the German Federal Office for InformationSecurity (BSI).

REFERENCES

[1]. D. Bernstein, E. Ludvigson, K. Sankar, S. Diamond and M. Morrow, *Blueprint for the InterCloud - Protocols and Formats for Cloud Computing Interoperability*, In Proceedings of the Fourth International Conference on Internet and Web Applications and Services, 2009.

[2]. A. Celesti, F. Tusa, M. Villari and A. Puliafito, *How to enhance Cloud architectures to enable cross-federation*, Cloud Computing (Cloud), 2010 IEEE 3rd International Conference on, Seiten 337 – 345, 2010.

[3]. GICTF, *Use cases and functional requirements for inter-Cloud computing*, GICTF White Paper, Global Inter-Cloud Technology Forum, 2010.

[4]. B. Farroha and D. Farroha, *Cyber security components for per- vasive Enterprise Security Management and the virtualization aspects*, Systems Conference, 2010 4th Annual IEEE, 2010.

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

[8]. J. Rhoton, *Cloud Computing Explained: Implementation Hand- book for Enterprises*, Recursive Press, 2010.