Towards User-Centric Management of Security and Dependability in Clouds of Clouds *

Marc Lacoste[1] and Fabien Charmet[2]

[1] Orange Labs, France
[2] Télécom SudParis, CNRS Samovar UMR 5157, France

Abstract. SUPERCLOUD aims to fulfil the vision of user-centric secure and dependable clouds of clouds through a new security management architecture and infrastructure. It will support user-centric deployments across multi-clouds enabling composition of innovative trustworthy services, thus uplifting Europe innovation capacity and competitiveness.

Keywords: clouds-of-clouds security, user-centric security, self-service security, self-managed security, end-to-end security, resilience.

Today, the cloud is moving distributed. However, the overall distributed cloud paradigm still remains highly provider-centric. Several major security and dependability challenges are ahead. First, *cloud layers* are extremely vulnerable to attacks spanning several layers (e.g., customer VMs, cloud provider services, provider hypervisor). The hypervisor is notably a target of choice due to its complexity. Hence the difficulty of an integrated protection. Second, *security management lacks flexibility and control*. The problem comes from heterogeneity of security components and policies between cloud providers. This has a strong security impact by introducing more vulnerabilities due to mismatching APIs and workflows. And third, *security administration challenges* remain. Manual administration of protection of such infrastructures is clearly out of reach to complexity and heterogeneity of their components. Automation of security management is clearly necessary but lacking today.

The SUPERCLOUD project [1] proposes new security and dependability infrastructure management paradigms for clouds of clouds. The security architecture will be *user-centric*: self-service clouds-of-clouds enable customers to define their own protection requirements and avoid provider lock-ins. Security will also be *self-managed*: self-protecting multi-clouds facilitate security administration thanks to automation.

* This paper is based on contributions from the entire SUPERCLOUD consortium. The project leading to this application received funding from the European Union Horizon 2020 Research and Innovation Program under grant agreement no. 643964. This work is supported (in part) by the Swiss State Secretariat for Education Research and Innovation (SERI) under contract number 15.0091.

"The camera-ready version of the paper has been published in the proceedings of the 6th International Conference on E-Democracy (http://www.edemocracy2015.eu/) and is available at Springer via: https://dx.doi.org/10.1007/978-3-319-27164-4_15 "

Approach: The project will build on the concept of *super-cloud* [2] as new architectural abstraction for distributed cloud security management. The super-cloud is a distributed management plane providing an end-to-end interface between user-centric and provider-centric views of multiple clouds (see Figure 1). It captures both distributed resource abstraction, and flexible but unified control for security and resilience across different clouds.

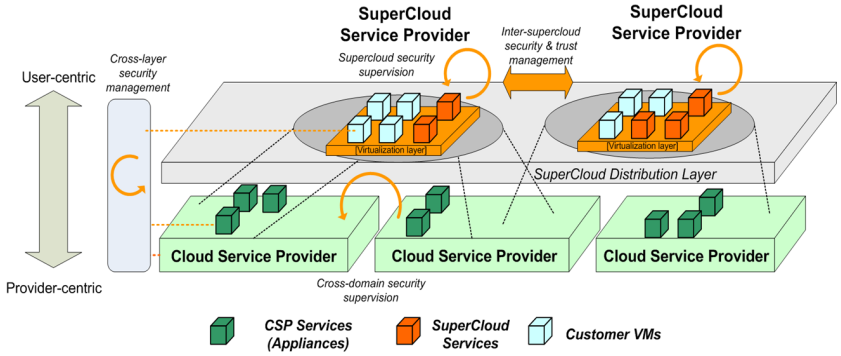

Fig. 1. Super-cloud architecture.

Objectives: SUPERCLOUD aims to achieve four key properties. First, *self-service security* through a cloud architecture giving users the flexibility to define their own protection requirements and instantiate policies accordingly. Second, *self-managed security* through an autonomic security management framework that operates seamlessly over compute, storage and network layers, and across provider domains to ensure compliance with security policies. Third, *end-to-end security* by proposing trust models and security mechanisms that enable composition of services and trust statements across provider domains. Finally, *resilience* through a resource management framework safely composing provider-agnostic resources using primitives from different providers.

Expected results: SUPERCLOUD will build a self-management infrastructure for security and dependability of heterogeneous resources across federated clouds. Customers will be provided with self-service environments enabling adaptive, customizable security for their cloud applications and services. SUPERCLOUD will also provide innovative cryptographic methods and tools for protecting data across distributed clouds through on-demand data security services, such as access control, blind computation, and data availability. Finally, SUPERCLOUD will enable resilient network-as-a-service, leveraging software-defined networking paradigms. It will provide strong guarantees for end-to-end security and integrated trust management across multiple infrastructure layers and cloud domains. The SUPERCLOUD core technology will be validated through testbed integration for real-world use cases in the healthcare domain.

References

1. SUPERCLOUD H2020 Project. `http://www.supercloud-project.eu/`.
2. Dan Williams, Hani Jamjoom, and Hakim Weatherspoon. Plug into the Supercloud. *IEEE Internet Computing*, 17(2):28-34, March 2013.