European Commission

SUPERCLOUD
User-centric management of security and dependability in clouds of clouds

SUPERCLOUD develops new distributed cloud security and dependability infrastructure management paradigms. Our approach is User-Centric for self-service clouds-of-clouds. We focus on Self-Managed services for self-protecting clouds-of-clouds reduce administration complexity through automation.

AT A GLANCE

Project title:
SUPERCLOUD – User-centric management of security and dependability in clouds of clouds.

Project coordinator
Dr. Klaus-Michael Koch
Technikon Forschungs- und Planungsgesellschaft mbH

Partners from:
France, Switzerland, Portugal, Germany, the Netherlands, Austria

Duration:
3 years

Total cost:
6.863.279,- €

EC Contribution:
5.398.280,- €

Programme:
Horizon 2020

Further information:
The project leading to this application has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 643964.
This work was supported by the Swiss State Secretariat for Education, Research and Innovation (SERI) under contract number 15.0025. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the Swiss Government.

Context and motivation

SUPERCLOUD aims to support user-centric deployments across multi-clouds, enabling the composition of innovative trustworthy services, to uplift Europe's innovation capacity and thus improve its competitiveness.
SUPERCLOUD will thus build a security management architecture and infrastructure to fulfil the vision of user-centric secure, dependable cloud of clouds.

Despite many benefits in terms of business, distributed cloud computing raises many security and dependability concerns. At stake are an increase in complexity and a lack of interoperability between heterogeneous, often proprietary infrastructure technologies.

Challenge

Provider-centric clouds currently face three major security challenges:

Security vulnerabilities in infra-structure layers
Each layer (e.g., customer VMs, cloud provider services, provider hypervisor) is extremely vulnerable to attacks. For instance, the hypervisor and its over-privileged Dom0 is a target of choice for attackers due to its complexity. Hence the integrated protection challenges.

Lack of flexibility and control in security management

Heterogeneity of security components and policies between providers has strong security impacts, with new vulnerabilities due to mismatching APIs and workflows.

Security administration challenges

Manual administration of infrastructure protection is out of reach due to complexity and heterogeneity of its components. Automation of security management is necessary, but lacks today.

Solution

The SUPERCLOUD project proposes new security and dependability infrastructure management paradigms that are:

User-centric

In self-service clouds-of-clouds, customers define their own protection requirements and avoid provider lock-ins.

Self-managed

Self-protecting clouds-of-clouds reduce administration complexity through security automation. Our approach is defining a new distributed architectural plane, **the SUPERCLOUD**, providing an end-to-end interface both between user-centric and provider-centric views of multiple clouds. Its role will be both to provide a distributed resource abstraction and flexible but unified control for management of security and resilience.

We will:

Design and realize a SUPERCLOUD security management infrastructure

This autonomic security management infrastructure features a 360° monitoring framework that captures both horizontal (multi-domain) and vertical (cross-layer) dimensions of multi-cloud systems. It monitors resource security and guarantees secure computation, storage and communications, also enabling a continuum of security services.

Design and realize a data management framework

It will rely on cryptographic tools that address multiple aspects including key management for access control, data availability and resilience, secure data computation and verifiability. It will also include a resilience framework allowing implementation of multi-cloud storage systems to survive provider-scale failures.

Design and realize a multi-cloud network management infrastructure

This includes a virtual network abstraction platform that spans multiple heterogeneous clouds and provides resilient Network-as-a-Service to cloud users. It serves as foundation to an autonomic security management framework that provides fine-grained network monitoring and flexible threat management support.

Expected impact

Self-Service Security

The SUPERCLOUD architecture will give users flexibility to define their own protection requirements and instantiate policies accordingly.

Self-Managed Security

The SUPERCLOUD autonomic security management framework will enable to operate seamlessly over compute, storage and network layers, and across provider domains to ensure compliance with security policies.

End-to-End Security

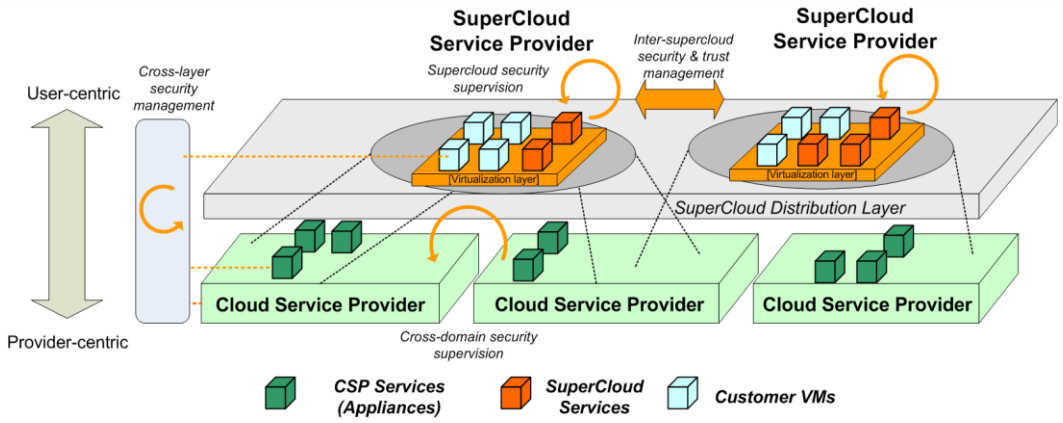
The proposed trust models and security mechanisms will enable composition of services and trust statements across different administrative provider domains.

Resilience

The resource management framework will enable to compose provider-agnostic resources in a robust manner using primitives from diverse cloud providers.

Healthcare Use Cases

The SUPERCLOUD methodology will be validated by testbed integration for real-world use cases in the healthcare domain.



Factsheet - SUPERCLOUD (GA no. 643964)