Research activities and innovative developments in European research institutes

# SECCRIT: Secure Cloud Computing for High Assurance Services

by Roland Bless, David Hutchison, Marcus Schöller, Paul Smith and Markus Tauber

***Owing to concerns about privacy, security and resilience, critical infrastructure service providers are not yet making wide-scale use of cloud computing for their high-assurance ICT services. The EU-funded SECCRIT project aims to address this problem so the benefits of the cloud can be leveraged in this sector in a safe and secure manner.***

Cloud computing is one of the most important and successful recent trends in consumer market service provisioning. According to the definition from NIST [1], it is an operational service model, wherein services are deployed on remote data centre infrastructures, which make use of virtualization technology. The use of virtualization enables rapid and flexible (elastic) service deployment. Attracted by the benefits of cloud computing, critical infrastructure providers, such as utility companies and government bodies, are considering deploying their high assurance ICT services in the cloud. However, privacy, security and resilience requirements are more stringent in this sector than in the general consumer market, thus hampering the wide scale use of cloud computing. In order to address these challenges, and enable the safe and secure usage of cloud computing for critical infrastructure ICT services, the EU-funded SECCRIT project has a number of objectives:

## Propose critical infrastructure cloud legal frameworks and guidelines

The project will identify the relevant European legal framework and establish respective guidelines for the use of cloud services in the critical infrastructure sector. Without establishing such a legal framework, the use of cloud in this sector, in which there are often stringent regulatory and legal requirements, will continue to be severely limited. Furthermore, it is important to have clear guidelines on how to address liability issues in light of service failures.

## Investigate and develop technologies for critical infrastructure cloud

Building on this legal framework, the project will investigate solutions for fault identification and localization using digital forensic methods [2] in cloud infrastructures. Attacks and failures are inevitable; therefore, it is important to develop approaches to understanding cloud behaviour in the face of challenges and attacks. In this area, we will investigate where are the appropriate points in the cloud to place monitoring and attack detection functionality. In order to contextualize the research in SECCRIT, we have derived an architectural model, shown in Figure 1, which represents our view that cloud computing needs to account for resilience, security and privacy concerns. A key task is to further develop this cloud architectural model to make it suitable for the critical infrastructure context, as current models are not well-

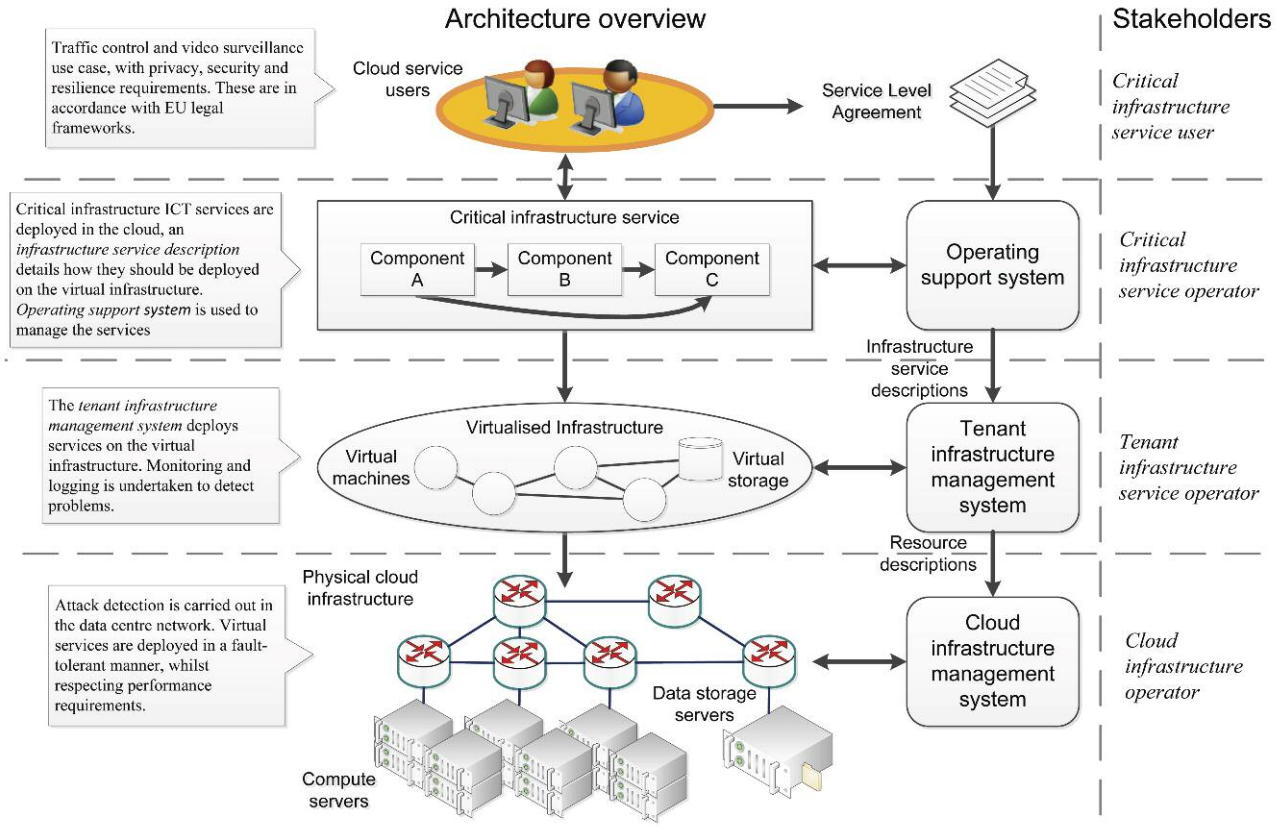


*Figure 1: Overview of the SECCRIT architectural model*

suited for use in this domain. For example, we have identified the need for a finer distinction between roles to reflect separation of administrative responsibilities and interfaces.

## Understand risks and provide best-practice guidance

A key challenge faced by potential critical infrastructure cloud users is to understand the new cyber-security risks associated with this technology. Despite some work in this area, eg, on understanding cloud-specific vulnerabilities [3], there is a lack of suitable techniques and processes for understanding and managing risk associated with cloud environments, which involves numerous stakeholders. This project aims to address this shortcoming. Building on all the aforementioned activities, the project will establish a set of best-practice guidelines for secure cloud service implementations, which can be used by the various stakeholders in this area to ensure secure and resilient cloud services. For instance, the guidelines can be used to determine the appropriate cloud deployment model for a service, eg, public, private or hybrid community cloud.

## Real-world evaluation and strong stakeholder engagement

In order to validate the project's outcomes, two demonstration deployments will be undertaken: (i) using the cloud to support a traffic management system in the city of Valencia; and (ii) implementing a video surveillance system that monitors critical infrastructures with the support of cloud-based services. Furthermore, the SECCRIT project has a growing user and advisory board, which provides requirements from various critical infrastructure domains and evaluates the project's outcomes. Members of the board receive privileged access to project results.

## About the project

The SECCRIT project started in January 2013 and will run for three years. It is funded by the European Union under grant number 312758. The consortium, coordinated by AIT, Austrian Institute of Technology (AT), is drawn from across Europe, and includes Amaris (AT), ETRA I+D (ES), Ajuntamente De Valencia (ES), Fraunhofer IESE (DE), KIT, Karlsruhe Institute of Technology (DE), NEC Laboratories Europe (UK), Lancaster University (UK), Mirasys Ltd. (FI), and the Hellenic Telecommunications Organization S.A. (GR). News, details about how to join the project's advisory board, and our deliverables can be found on the project web site.

**Link:** https://www.seccrit.eu

**References:**

[1] P. Mell, T. Grance: "The NIST Definition of Cloud Computing, NIST Special Publication 800-145," September, 2011.
[2] T. V. Lillard: "Digital Forensics for Network, Internet, and Cloud Computing: A Forensic Evidence Guide for Moving Targets and Data," Syngress Publishing, 2010.
[3] B. Grobauer, T. Walloschek, E. Stocker: "Understanding cloud computing vulnerabilities," IEEE Security & Privacy, vol. 9, no. 2, pp. 50–57, March-April, 2011.

**Please contact:**

Markus Tauber
AIT Austrian Institute of Technology / AARIT, Austria
Tel: +43 664 8251011
E-mail: seccrit@ait.ac.at