Certifying Services in Cloud:

The Case for a Hybrid, Incremental and Multi-Layer Approach

George Spanoudakis
City University London, UK

Ernesto Damiani
University of Milan, Italy

Antonio Maña
University of Malaga, Spain

(Extended Abstract)

I. Motivation

Cloud technology offers the opportunity for efficient utilisation of resources from offering compute, data, storage, and network capabilities as services on demand. However, it also raises significant concerns regarding the security, privacy, governance and compliance of the data and services offered through it. This is because the deployment of software applications and data through cloud infrastructures introduces several security problems, including compromises of integrity, confidentiality [3][4] and/or privacy of customer data on clouds [4][6]; software protection [10]; reduced application and data availability [2][5][3]; and authentication, authorization and accounting (AAA) vulnerabilities [3]. Also, current cloud infrastructures have opaque service offerings where users cannot monitor the underlying physical infrastructure..

Security and compliance verification in clouds are tricky as security can be affected by interference between features and behavior of all the inter-dependent services at any of the layers in the cloud stack as well as by dynamic changes in them [3]. Dynamic changes in the data isolation scheme operated by a cloud may, for example, affect the privacy of the data processed by a software service in the same cloud, compromising the service's compliance to an organizational privacy policy or, worse, to a law or a regulation. Similarly, changes in cloud messaging services at the platform layer may affect the availability and/or reliability of the software services that rely on those messaging services. The same may happen to non-repudiation properties as, for example, compromising the services' compliance to an internationally acknowledged certified messaging scheme like *Universal Postal Union*.

Run-time changes affecting service (or process) properties may create unexpected and unwanted liabilities, as final users of services may hold the service supplier responsible for failing to withhold properties, even if violations have been caused by dependencies between the services and the cloud where they are executed. Such dependencies do not cause only bottom-up effects. Inefficiencies of software services, for instance, may affect overall cloud performance and denial-of-service attacks to specific services at the software layer may affect availability of services at all other layers in the cloud stack.

The risk arising from such dependencies is exacerbated by the absence of common ownership and the evolving population of services at all layers of a cloud. Hence, in current realizations of cloud computing there are no guarantees that there will be no interactions between cloud service features that may cause security vulnerabilities and violations of security properties, even if pre-operational verification tests have been performed [3][5].

A common approach to enhancing assurance and reducing risks in such settings is to rely on the certification of different services in clouds. Certification has a long history as a mechanism for verifying properties and increasing trust in software systems. While traditional certification techniques apply mostly to monolithic systems, recent research demonstrates the feasibility of security certification for service based systems and processes [11]. Research on service certification has focused on the use of certificates at design time, without addressing the question of how to certify inter-dependent software services running at all layers of the cloud stack. Also, existing approaches do not support certification combining different types of evidence, including static verification, testing, monitoring and trusted computing proofs for services at all layers of the cloud stack.

II. Novel Cloud Certification infrastructure

To address these limitations we are developing a novel *Certification infrastrUcture for MULti-layer cloUd Services* (CUMULUS). This infrastructure will provide models, processes and tools supporting the certification of compliance and security properties of all types of cloud services, i.e., infrastructure (IaaS), platform (PaaS) and software services (SaaS), through the use of *multiple types of evidence* including testing, monitoring and trusted computing proofs. It will also support *incremental certification*, if necessary.

The utilisation of multiple types of evidence for producing security certificates is necessary as the assessment of certain security properties in clouds might be possible only through a combination of such evidence types. Trusted Computing Platform (TCP [1]) proofs, for instance, can assess the trustworthiness of the lower hardware level of the cloud stack. Consequently, combining certificates underpinned by TCP proofs with others based on testing and monitoring provides a comprehensive trust chain for covering further properties as well as hierarchically dependent services in higher layers of the cloud stack.

The integration of results of different types of evidence requires novel *hybrid certification models* supporting the identification of gaps arising from evidence from a specific verification method (testing/monitoring/TCP) and finding ways of filling them by evidence from other methods. Test based certificates of software services that have been issued under certain operational conditions can, for example, be combined with monitoring data acquired in cases where the related conditions are violated to produce extended hybrid certificates for the properties of interest. Also, the test plan that has been used to produce the original certificate may provide the basis for assessing the length of monitoring activity required to validate the certificate under new conditions at run-time. Similarly, a hybrid certification model may support the combination of evidence coming from TCP-proofs with other testing and/or monitoring based certificates. A TCP proof can, for instance, provide evidence that an infrastructure configuration upon which a service instance runs is the same as the one for which the service was originally tested. Suppose, for example, that a service holds a test based certificate asserting a data integrity property if the service runs on an infrastructure that does not support multi-tenancy. Then, the existence of a formal TCP proof for single tenancy becomes a necessary pre-condition for verifying the applicability of the test-based certificate. In certain cases, integration of evidence requires the ability to combine existing certificates and freshly acquired raw evidence from all layers of the cloud stack to produce composite certificates (*multi-layer certification models*).

The CUMULUS infrastructure supports also *incremental certification*. Incremental certification is needed to address a major limitation of traditional certification processes, namely their inability to cover changes that affect certified properties without having to re-certify from scratch. Incremental certification can be supported by continuous monitoring of cloud services to ensure the validity of previously verified properties following changes in the stack (e.g., deployment of new middleware and service instances). Certification based on continuous monitoring can achieve an awareness of the operational context that is hard to obtain with static certification techniques such as testing [8].

A conceptualization of the CUMULUS infrastructure is shown in Figure 1. The infrastructure includes: (a) security and certification models; (b) components producing core test, monitoring and trusted computing based certifications as well as multi-layer and components producing incremental and hybrid certifications (c) components providing certification related evidence from clouds (test and monitoring services and trusted computing platforms); (d) an interaction protocol for the provision of certification evidence; and (e) tools supporting the engineering of cloud services that can make use of the infrastructure. The infrastructure can be used by cloud certification authorities to generate certificates for SaaS, PaaS and IaaS services. Cloud service providers may also use it for self-certification and building services amenable to the types of certification supported by it. The development of CUMULUS infrastructure is the focus of a new FP7 European project.

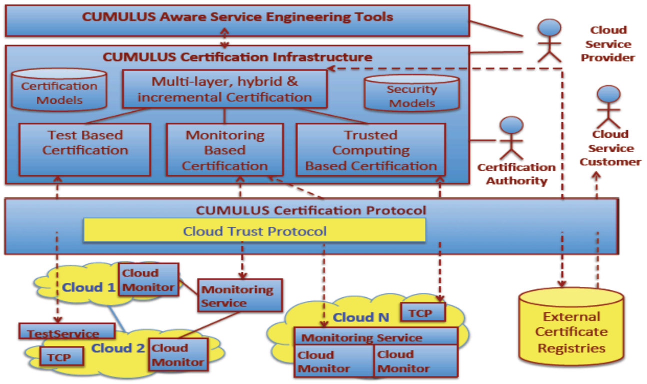

Figure 1: CUMULUS infrastructure

Our certification-based approach is in line with emerging audit approaches based on logging and reporting of cloud operations [2][8] (e.g., GRC Stack and Cloud Trust Protocol [7]) and provides an evidential basis for assessing cloud security. However, it extends such approaches by focusing on the development of automated assessment schemes utilising operational evidence in association with online and offline cloud service tests and formal proofs of compliance. Furthermore, CUMULUS's focus on certificate-based security assessment enables the establishment of clear liabilities in the overall process.

REFERENCES

[1] Trusted Computing Group: TCG Specifications. Available online at. https://www.trustedcomputinggroup.org/specs/

[2] A. Haeberlen. "A case for the accountable cloud.", *SIGOPS Oper. Syst. Rev.* 44(2): 52-57, April 2010.

[3] D. Catteddu and G. Hogben, "Cloud Computing: Benefits, Risks and Recommendations for Information Security.", European Network and Information Security Agency (ENISA), 2009

[4] L. Kaufman. Data Security in the World of Cloud Computing. *IEEE Security and Privacy* 7, 4: 61-64, July 2009.

[5] M. Jensen, et al., On Technical Security Issues in Cloud Computing. In *Proc. of the 2009 IEEE Int. Conf. on Cloud Computing* 2009

[6] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing v2.1, available from: http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf

[7] Cloud Security Alliance, Cloud Security Alliance GRC stack, available from: https://cloudsecurityalliance.org/research/grc-stack/

[8] K. Dempsey et al., Information Security Continuous Monitoring (ISCM) for Federal Systems and Organisations, NIST Special Publication 800-137, Sep 2011

[9] European Commission, Cloud Computing: Public Consultation Report, Brussels, 5 Dec 2011, available from: http://ec.europa.eu/information_society/activities/cloudcomputing/docs/ccconsultationfinalreport.pdf

[10] A. Maña. Beyond Data Protection: Securing Software in Cloud Computing. Position paper at MMM-ACNS'10, Sep 2010.

[11] J.C. Pazzaglia, et al., Advanced Security Service cERTificate for SOA: Certified Services go Digital!, Proc. of Information Security Solutions for Europe (ISSE 2010)