# SEPRICC: Security and Privacy in Cloud Computing

Special Session along with CLOUD COMPUTING 2017, February 19-23, 2017 - Athens, Greece
The Eighth International Conference on Cloud Computing, GRIDs, and Virtualization
http://www.iaria.org/conferences2017/CLOUDCOMPUTING17.html

Sokratis K. Katsikas, Center for Cyber & Information Security, Norwegian University of Science & Technology (NTNU) - Gjøvik, Norway sokratis.katsikas@ntnu.no

Costas Lambrinoudakis, Department of Digital Systems, University of Piraeus, Greece
clam@unipi.gr

*Abstract*— **One of the new computing paradigms that has gained tremendous momentum in the past few years is cloud computing. This is due, at least to some extent, to the fact that IT cost reduction is achieved by offloading data and computations to cloud computing. Even though cloud computing as an economic model has found versatile ground and is attracting a lot of investment, many are still reluctant to use cloud services because of several security, privacy, and trust issues that have emerged.**

**The initial reaction of the security community to the security issues of cloud computing was that these could be resolved using existing techniques inherited from conventional IT systems or even distributed systems that are the ancestors of cloud computing environments. Unfortunately, this approach does not work, because of the scale and the architecture of the cloud computing model. Hence, a need to re-consider security, privacy and trust concerns in the context of the cloud computing paradigm arises.**

**In answer to these concerns, the Security and Privacy in Cloud Computing (SEPRICC) special session within Cloud Computing 2017, held in Athens, Greece, will provide an international forum for researchers and practitioners to exchange information regarding advancements in the state of the art and practice of security, privacy and trust in cloud computing.**

***Keywords— Cloud Computing; Security; Privacy.***

## I. CLOUD ENVIRONMENTS AND SECURITY

The ongoing financial crisis and the increasing computational and storage needs, have imposed severe changes to the modern IT infrastructures. IT cost reduction is achieved by offloading data and computations to cloud computing. Cloud services vary from data storage and processing to software provision, posing requirements for high availability and on-demand commitment-free provision of services. Cloud computing is usually thought as a secure environment that can provide infrastructures, services and processing power on demand. Its two main characteristics are:

- Scale: In order to achieve significant savings, the cloud model supports massive concentrations of hardware resources for the provision of the supported services,
- Architecture: Although customers who share hardware and software resources are typically unrelated, they rely on logical isolation mechanisms to protect their data. Computing, content storage and processing are massively distributed. This tendency towards global distribution and redundancy means that resources are usually managed in bulk, both physically and logically.

Even though this economic model has found versatile ground attracting a lot of investments, many people and companies are reluctant to use cloud services because of several security, privacy and trust issues that have emerged. The aforementioned two characteristics of Cloud Computing are at the heart of the cloud's security, privacy and trust issues that have emerged. For instance, as far as scale is concerned, Cloud Computing infrastructures have massive concentrations of computational resources. Consequently, in case of a security incident the impact will be more severe than that met in ordinary IT and distributed systems. Regarding the cloud architecture, although cloud providers promise physical and logical isolation to their customers, it is rather difficult to achieve it since most of the time they share the computational resources of the same physical machine, either using cloud services or Virtual Machines (VM) [1]. It is therefore clear that new security and privacy issues are raised.

According to [2], [3], [4], [5], [6], [7], [8] the most important security issues in cloud computing are: trust, integrity, availability, authentication and authorization, and confidentiality. ENISA [1] has also investigated the different security risks related to the adoption of cloud computing along with the affected assets, the risks likelihood, the potential impact, and the vulnerabilities in cloud computing that may lead to such risks. In [9] the security vulnerabilities of a cloud platform are discussed. Furthermore, [10]

compares existing information security frameworks that have been specifically designed for Cloud Computing environments using the clauses from the ISO/IEC 27002 standard as evaluation criteria.

In order to address the new security issues there is also research work on the design and implementation of cloud specific security frameworks and architectures. In [11] a cloud security scheme that emphasizes on the architecture and on the interaction between different services is proposed. Cloud specific security measures can also be found in [12]. The National Institute of Standards and Technology (NIST) [13] framework provides a set of activities in order to identify threats, protect assets, detect attacks, respond and recover from incidents, thus facilitating the implementation of an overall security solution.

## II. Understanding the Threats

In order to address the new cloud computing security threats, it is important to understand their uniqueness as compared to other threats met either in conventional IT systems or distributed systems. To this direction the information provided by two security organizations, those of ENISA[1] and Cloud Security Alliance [14] are utilized.

ENISA a few years ago presented a survey of Security in Cloud Computing systems. This survey begins by analyzing the benefits of Cloud Computing systems. However, even though there are benefits in terms of scale and resource concentration, when it comes to the top security threats session it is clear that the benefits are outnumbered. The same survey makes a classification of threats and separates them into policy and organizational threats, technical threats, legal threats and threats not specific to the Cloud. Each threat is assigned a grade which varies from low to high and is defined according to its probability, impact, vulnerabilities and affected assets.

It must be stressed that the threats which are not cloud-specific form only one category of threats and are fewer than all the others. As a result, the manifestation of Cloud Computing systems has created a whole new world of security threats that were unknown in the past. Excellent and representative examples are isolation failure, which refers to the lack of logical isolation, and Economic Denial of Service, which refers to exhaustion of computational resources of a cloud system in purpose by a customer, so as to make the cloud provider unable to serve other customers. Another notable case is the malicious insider, a concept redefined in the context of Cloud Computing Systems. The survey also pays attention to the vulnerabilities, briefly explaining each element of the provided categorization. Once again the vulnerabilities that are not cloud-specific are fewer than those generated by the existence of cloud systems.

Cloud Security Alliance supports that, despite the similarities in security controls between IT environments and Cloud systems, there are a lot of differences in the threats taken by an organization. Cloud services employed, operational models and the technologies used to employ Cloud services are the sources of the new threats. Furthermore, it is noted that there are differences in the security responsibilities of the provider and the consumer among cloud service models. In addition to that, as cloud providers aim at cost efficiency, thus achieving scale, reuse and standardization they come up to the point where security mechanics lose their flexibility.

Both ENISA and Cloud Security Alliance refer to customers and simple users of Cloud systems who may become one of the greatest threats along with users with elevated privileges. Compared to traditional IT services, the cloud attack surface has expanded, not only because of the shared resources but also due to the additional attack vectors that an adversary may utilize for exploiting a potential vulnerability in the VM, in the cloud management platform, or in any other component of the cloud infrastructure. As a result, the "Malicious Insider Threat" has evolved to one of the greatest security challenges in cloud computing environments.

## III. Security and Privacy in Cloud Computing (SEPRICC)

The special session of SEPRICC comprises of three research papers that tackle cloud computing security and privacy issues. The first paper (*Security and Privacy Requirements Engineering Methods for Traditional and Cloud-Based Systems: A Review*) presents an overview and compares a number of well-known security and privacy requirements engineering methods applied in traditional and cloud-based systems in order to reveal the existing gaps in the specific research field and propose a number of criteria that should be addressed for successfully capturing and modeling security and privacy requirements. The second paper (*Trust Managemement Parameters in Cloud Computing Environments*) addresses the issue of trust form cloud providers to clients and vice versa. It identifies and proposes a set of parameters that can be utilized in order to quantify the trust level of the cloud provider to the client. The final paper (*The Greater The Power, The More Dangerous The Abuse: Facing Malicious Insiders in The Cloud*) proposes an intrusion detection method for cloud environments, based on the monitoring of hypercalls. More specifically it monitors the deployed virtual machines operations, correlating the collected information to detect uncommon behavior based on the Smith-Waterman algorithm.

## IV. References


[1] ENISA, "Cloud Computing – Benefits, risks and recommendations for information security" (2009).

[2] KSHETRI, N. (2013) Privacy and security issues in cloud computing: The role of institutions and institutional evolution. Telecommunications Policy, 37, 372-386.

[3] ALMORSY, M., GRUNDY, J. & IBRAHIM, A. S. (2011 ) Collaboration-Based Cloud Computing Security Management Framework. IEEE 4th International Conference on Cloud Computing.

[4] LOMBARDI, F. & DI PIETRO, R. (2011) Secure virtualization for cloud computing. Journal of Network and Computer Applications, 34, 1113-1122.

[5] STINCHCOMBE, N. (2009) Cloud computing in the spotlight. Infosecurity, 6, 30-33.

[6] MANSFIELD-DEVINE, S. (2008) Danger in the clouds. Network Security, 2008, 9-11.

[7] SUBASHINI, S. & KAVITHA, V. (2011) A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34, 1-11.

[8] ABDUL NASIR KHAN, M.L. MAT KIAH, SAMEE U. KHAN & MADANI, S. A. (2013) Towards secure

mobile cloud computing: A survey. Future Generation Computer Systems, 29, 1278- 1299.

[9] B. Grobauer, T. Walloschek and E. Stöcker (2010) Understanding Cloud-Computing Vulnerabilities, IEEE Security and Privacy, vol. 99.

[10] Rebollo, O., Mellado, D., F-Medina, E. (2011) A Comparative Review of Cloud Security Proposals with ISO/IEC 27002, Proceedings of the 8th International Workshop on Security in Information Systems, pp.3-12.

[11] S. Pal, S. Khatua, N. Chaki, S. Sanyal (2011) A new trusted and collaborative agent based approach for ensuring cloud security, arXiv Preprint arXiv:1108.4100.

[12] E.B.Fernandez, Raul Monge, and Keiko Hashizume (2015) Building a security reference architecture for cloud systems, Requirements Engineering.

[13] NIST, Framework for Improving Critical Infrastructure Cybersecurity (2014) Technical Report, Version 1.0, February.

[14] Alliance, C. (2011) Security guidance for critical areas of focus in cloud computing v3.0, Cloud Security Alliance.