Securing the cloud: A trust, risk and security centric view of a enterprise's use of cloud computing services

Full Day Tutorial at IFIPTM 2011, Tuesday 28 June, 2011

Technical University of Denmark, Anker Engelundsvej 1, Kgs. Lyngby

Tutorial Summary

Cloud computing has emerged as one of the most promising and challenging IT technologies of our time. This new paradigm utilises two separate technological development—utility computing and service oriented architecture—to provide the users (individuals, SMEs and enterprises) with a highly scalable, pay-per-use,   everything-as-a-service model for IT delivery. The characteristics of cloud give rise to several business drivers that make cloud computing an attractive service delivery model from a customer's point of view. Customer expectations include capital expenditure reduction, increased IT agility, faster return on investment and removal of barriers to entry as well as a more robust and resilient infrastructure leading to improvements on business continuity.

However, cloud technology has also brought to forefront questions related to risk, security and trust both from an academic and an industrial perspective.

In this tutorial we will analyse the main trust and security related concerns associated the use of cloud-based resources and consider solutions to solving the identified problems. In particular we will look at how issues related to security, risk, trust and service level agreements can be systematically evaluated to identify the salient issues at play and to come up with a framework for evaluating the impact of these issues and for solving them.

In particular we will analyse the following key areas:

- The applicable risk model for use in a cloud based shared resource infrastructure
- The issues related to trust within a cloud based ecosystem
- The security related to various aspects of the cloud, including the infrastructure and data
- The service level agreements and its relevance in the context of the cloud based delivery model

Areas in detail

Security

Security is a big consideration when enterprises consider moving their IT processes to the cloud. The perceived loss of control over process and services along with the concerns over confidentiality of corporate data, privacy, integrity and availability of services and data act as significant showstoppers preventing Corporations and SMEs from using cloud based services.

In this session we will

1. Focus on some of the major security challenges and aim to provide recommendations, based on the work of international expert groups by the European Network and Information Security Agency and the Cloud Security Alliance among others

2. Summarise the research and innovation roadmap put forward by a major technology and service provider

3. Demonstrate innovative emerging technologies relating to virtualisation and cloud security

4. Present best practises on cost efficient solutions to mitigate the security concerns relating to the use of cloud by Enterprises and Government.

Trust

A reliable Cloud service eco-system depends, in part, in the establishment of a trustful relationship between Cloud Service Providers and Service Customers. The open and self-service nature of Cloud Services should be characterized by its high dynamicity, allowing customers to dynamically switch or to combine seamlessly different providers. In the context of Cloud Service provision, we can interpret Trust as the positive belief that a specific provider's service will satisfy the expectations of a particular consumer based on the agreed service level. This is the degree in which a provider satisfies the terms agreed parameters for the provision of a service to the Customer. The trust between customer and the cloud provider grows from their experience working together for a certain period. To calculate and enforce this bilateral relationship there are a set of parameters from both points of view, such as the SLA violations, the amount of resources needed by a service or security mechanism, reliability or location (country were the provider is registered) as the legal aspects about data protection is one of the main issues when we talk about cloud computing. In the case of the end-user, its relation is with the SP and here is where the main issue comes.

In this tutorial session, among others, we will analyse the:

- The concept of Trust from the points of view of Cloud customer and Infrastructure Provider.

- Transfer of models from social networking to evaluate and build trust between entities in the ecosystem.

Risk

This session will discuss a risk assessment framework that defines a risk inventory for use of cloud based infrastructure services, facilitates the assessment of risk for service deployment and enables the providers to identify infrastructure bottlenecks and manage risk associated with SLA violations. It includes risk identification, assessment, treatment, and monitoring for systematic risk, uncertainty or non-systematic risk, as well as probabilistic risk.

Trust and Risk elements of Service Level Agreements

Current Cloud environments are offered to their customers in a best effort approach. In contrast, both customers and service provider intending e.g. to extend their own resources dynamically with Cloud resources, e.g. in case of peak demands, need reliable Service Level Agreements with the Cloud infrastructure provider. This Service Level Agreement can cover aspects like trust, risk, cost, security, legal requirements for data-placement, eco-efficiency and more.

This session of the tutorial will give an overview on approaches for negotiating and creating Service Level Agreements and cover term languages used to express properties of parameters like trust, risk etc.

Registration

Registration for the tutorial is necessary and online registration is possible through the IFIPTM 2011 web-site (http://ifiptm.org/IFIPTM11/Registration.html).

About the tutors

We have put together a list of tutors covering the academy, research institutions, and the industry. These include faculty of University of Leeds, Fraunhofer Institute for Algorithms and Scientific Computing SCAI, ATOS Origin and BT Innovate and Design. *We are also hoping to confirm tutors from European Network and Information Security Agency and Cloud Security Alliance.*

Dr. Theo Dimitrakos is the Head of Security Architectures Research in the Security Futures Practice of BT Innovate & Design (I&D). He has fifteen years of experience in a range of topics relating to Information Security, Identity and Access Management, Service Oriented Architecture (SOA), Web Services and Grid Computing. He is involved in the Cloud Security Strategy definition at BT I&D and also part of the European Network and Information Security Agency (ENISA) expert advisory group working on Cloud Security Risk Analysis. Theo has been the scientific coordinator of some of the largest and most successful research initiatives in EU, such as BEinGRID (2006-10), which includes 96 partners and oversees 25 business pilots in different market sectors; and the TrustCoM (2004-07) that brought together teams from Atos Origin, BT, Microsoft, IBM and SAP, among others

Srijith K. Nair is a Senior Researcher in the Security Futures Practice of BT I&D and is currently looking at security issues related to virtualisation and the cloud computing delivery model and other security issues involving SOA/SOI themes. He has been part of multiple expert groups advising European Network and Information Security Agency (ENISA) on the impact of cloud computing on the resilience of eGov services as well as on cloud computing security assessment and was also a part of the working group of the Cloud Security Alliance (CSA) delivering the security guidance report. He is also currently leading work package activities in "OPTIMIS," an EU funded three-year, €10.5m research and development project related to use of cloud based services.

Dr Karim Djemame is a Senior Lecturer within the Institute for Computational and Systems Science (I-CSS) at the School of Computing, University of Leeds. He was investigator of the DAME project and its follow-on BROADEN project. He was also the Leeds investigator and technical manager of AssessGrid project and the EPSRC follow-on-fund project "Grid Applications Performance Prediction Tool". He sits on a number of international programme committees for Grid middleware, computer networks and performance evaluation, and is an Associate Editor of the International Journal of Systems Science. The main research area of Dr Djemame is Cloud computing, including system architectures, resource management, performance evaluation, and risk assessment.

Wolfgang Ziegler is head of the Grid Middleware Research Group of the Bioinformatics department of SCAI and has a long record in HPC and Grid R&D. He has been active in the US Grid Forum and later the Global Grid Forum since 1999. He was a co-chair of the Global Grid Forum (GGF) GRID Scheduling Dictionary Working Group and he is a co-chair of the Open Grid Forum Grid Resource Allocation Agreement Protocol Working Group responsible for the WS-Agreement specification. He was member of the executive committee of the CoreGRID Network of Excellence. He is the scientific co-ordinator of the SmartLM project.

Juan Luis Prieto Martínez: B.S. in Business Computing Engineering by the Univeridad Rey Juan Carlos in Madrid (2006). He works in Atos Origin since January 2010 at Atos Research & Innovation. He has been working in research projects since 2006 in many different topics such as software quality, security (access management) and now, since he joined Atos his main focus has been in the Cloud Computing area where he works in different collaborative projects within Spain, NUBA (Normalized Usage of Business-oriented Architectures) and the EU commission in Optimis (Optimized Infrastructure Services).