

Title session

Can the Cloud be trusted

Responsible caretakers:

Volkmar Lotz, Jim Clarke, Nick Wainwright, Michel Riguidel

Other contributors to organisation of session:

Gregory Lopez, Volker Fusenig, Elmar Husmann, Demosthenes Ikonomou.

Name of Chair/rapporteur

Chair: Volkmar Lotz, SAP Research

Rapporteur: Jim Clarke, Waterford Institute of Technology, Nick Papanikolaou, HP LABS.

Session objectives

In this session, the main objective is the closer examination of Trust in a Future Internet (FI) that is made up of numerous solutions based on new paradigms of service offerings, including those in the context of cloud computing. One of major properties expected of the FI is to provide a platform for new businesses, which can only achieve value if there is sufficient trust in the infrastructures. The 'cloud', in its different appearances as infrastructure / resource cloud, platforms as a service, or applications as a service, exemplifies potential trust challenges, which the session was designed in order to be examined in greater detail, including:

- How can trust be built in the digital space of the cloud, where services and resources are exposed instead of humans? We do have means at hand (Service Level Agreements (SLAs), monitoring and logging, privacy enhancing technologies, reputation systems, security technology, process and risk models, etc.), how should they be combined and applied to manage trust effectively?
- Is trust specific to application domains and cloud models?
- What kinds of events in the cloud (like migration of data across servers or domains) have an impact on trust? What needs to be signalled to a user, taking his role as consumer or provider of services and content into account, how much details needs to be exposed?
- What needs to be done to ensure that users are not overwhelmed by the amount of information and technical detail, still being able to make informed decisions?
- Does the cloud need regulation to provide trust? Do cloud providers and services need to be certified? Which principles should apply?

The challenges in the session were addressed from two complementary angles and the speakers were chosen accordingly: a business viewpoint emphasizing on needs and customer requirements, and a technology viewpoint, emphasizing on technology enablers and the state of the art.

Presenters/title/organisation

Presenter	Title	Organisation
Gregory Lopez	Business View On Cloud Security	Thales
Volker Fusenig	Security Challenges For The Cloud	Fraunhofer Institute for Secure Information Technology
Elmar Husmann	Trustworthy Clouds In The Future Internet	IBM

Summary of presentations

Presentation 1. Business view on Cloud Security

The first presentation concerned a number of cloud platforms that had been developed by Thales for use by the French government and industry. By discussing examples of real systems, the speaker was able to illustrate the core security issues that emerge in the cloud.

An e-Health cloud platform for assisted living was presented; this is intended as a tool that facilitates the provision of healthcare and patient monitoring in their homes. In this example, there are very strict regulatory requirements that must be satisfied, and the success of the system is very sensitive to negative public perception.

Other examples of systems developed by Thales were specialized platforms for the French Ministry of Finance and for the French Ministry of Defense (MOD). These examples highlighted the need to ensure the privacy of citizens through secure access to personal data. The system for the French MOD is built on a private cloud, designed so that data held will not leave the country of collection at any time, even though interactions with other information systems abroad may be needed for processing. The core challenges faced by the developers of the system are managing the location of the data and providing mechanisms for secure federation and monitoring.

Broader challenges related to data security in the cloud include:

- who can access the data?
- when can data be accessed and under what conditions?
- what is the appropriate SLA?
- Can a user stop their contract at any time (reversibility)?

Compliance with security standards and privacy laws is a central requirement. To ensure compliance, clouds must incorporate data handling and monitoring mechanisms that guarantee the location of data, that can be checked and certified on a regular basis, that provide audit trails for data disclosures. Also, it is important to deal with issues like suppression of data and administering a managed requisition process for the data.

After the examples were presented, the speaker discussed the lessons learned and argued that there are still some open problems. It had become clear that service-level agreements would

have to be contractual and embedded within any cloud service offering, with cloud providers competing to provide the highest quality of service and availability.

Cloud providers have to deal with multi-tenancy issues and intrusions. Different customers are likely to be using the same physical infrastructure to host their systems and it is very difficult to guarantee 100% isolation of one system from another. There is a host of threats posed by this situation, including data losses and leakages as shared memory and shared Virtual Machines (VMs) are used.

One of the security and privacy challenges faced still by providers of cloud offerings include finding ways of enforcing compliance with applicable law and regulations. Since cloud operations involve data centers in multiple locations, dealing with flows of data between them all the while ensuring compliance is a core problem. Of course, it is also true that regulations on privacy, data retention and data access by law enforcement agencies are not always coherent and need to be brought in alignment with each other, thus making enforcement and automation of compliance practical and efficient.

Especially for government-grade applications, one will expect to get the same level of security provided by traditional solutions (and classical, closed infrastructures) from cloud platforms, but this seems very difficult to achieve at the moment. This is the most important challenge faced by cloud operators; they will need to provide ever higher grades of security than ever before to convince customers to migrate to their systems.

Presentation 2. Security Challenges for the Cloud

The presentation focused on cloud networking security for Scalable and Adaptive Internet Solutions (SAIL), a project engaged in R&D of novel networking technologies to lead the way from current networks to the networks of the future including one built of a cloud computing physical infrastructure.

First, the architecture for cloud networking was discussed, along with the scenarios and use cases in which cloud networking is of benefit. For instance, the deployment of virtual desktops is an enabler for the *dynamic (virtual) enterprise*. In this scenario, a thin client is connected to the virtual network infrastructure, and a virtual machine is provided to the user for his computing needs. Interestingly there is the challenge of reducing latency, since the virtual machine may end up being run on a physically distant machine, and this means there is a delay to network switching/routing processes.

Now, consider the SAIL scenario in which there are virtual machines hosted at different locations, which must all be interconnected through virtual networks. Users require access to some of these VMs and some of these networks, so there is the challenge of separating/isolating them from one another for security reasons. VMs at different locations need to be migrated to a closer location to the user to reduce latency, but to reduce network load they should be migrated where network availability is high; these requirements may be conflicting at any given time. Furthermore, there is the fundamental issue of cost, which places a requirement to run VMs on the cheapest possible infrastructure. Such are the challenges that SAIL attempts to address.

A practical scenario where the very same problems arise while running on a cloud infrastructure is that of *intelligent video distribution*. For a video to be distributed effectively, the cost of distribution should be low while at the same time ensuring quality of service, so that frames are not lost (which would be damaging to the experience of the user).

For cloud networking, there is the central question of where and how to perform virtualization management. Where exactly, on a large, physically distributed network of interconnected virtual links, would a given VM be run? Which machine would host the hypervisor and what policies would it need to enforce? All of these issues were raised during the talk.

Clearly, there is a need for new policy models and policy enforcement mechanisms for cloud networking. There are different tradeoffs to consider, as well as the issue of cross-border data flow. New encryption mechanisms are likely to be needed, in particular for secure channels along particular links. Homomorphic encryption might in principle work as a means of processing encrypted data, but it is not yet widely available in a practical form. There is an element of trust that inevitably needs to be placed on cloud providers.

In summary, cloud networking is a framework that combines cloud computing and virtual networking; this requires combined control of computing and network resources. Cloud networking enables flexible usage of virtual infrastructures via the live migration of VMs between different locations, and subsequent optimisation of VM placement given constraints on latency, network load and cost. The use of cloud networking is likely to enable new business models and will in particular fuel the virtual enterprise. For this to happen, of course, there are key security challenges need to be better understood and then resolved.

Presentation 3. Trustworthy clouds in the Future Internet

This talk began with some shocking statistics, which of course are intended to demonstrate the significance of security measures for cloud platforms. It seems that in a particular study, 80% of enterprises consider security issues the key inhibitor to adopting cloud-based solutions for their business. The same study showed that only about 48% of enterprises were as concerned about reliability. This shows that industry would be willing to have some tolerance with regards to quality of service, but much less so with confidentiality of their systems and data.

There are of course different types of cloud – private, public and hybrid clouds. The speaker asked which type of cloud is suitable for what. The risk concerns include control, reliability, compliance, data handling and security management (by whom, when, where?). There are trust and security limitations for global cloud infrastructures, due to the openness of these platforms to all sorts threats.

IBM projects on cloud platforms have included RESERVOIR and VISION; the challenges raised by these projects include the following. First, there is the question of how to federate public clouds; there is also the issue of moving data from one cloud to another. Privacy issues are very worrisome and have yet to be addressed fully. Other practical problems have included preventing data leakage from one customer to another, and restricting the damage that one cloud customer/user can inflict on the others (especially when sharing the same infrastructure).

There are threats posed by cloud administrators, who are capable of performing insider attacks. While in traditional systems, system administrators have wide privileges, they domains within

which they operate are clearly demarcated; this may not be the case in the cloud setting, due to the fact that systems are inherently distributed and difficult to pin down and restrict: data flows across administrative and physical domains.

Another difficulty with cloud platform offerings is the lack of transparency and hence, of understanding on the side of the customer. There is what is known as the *cloud curtain*, a term which refers to the manner in which cloud providers hide the details of how a cloud service is technically delivered to customers. The consequence of this is that customers cannot gain any insight into real system status and how to deploy adequate risk mitigation mechanisms. Certified, auditable cloud services are likely to provide higher levels of trust. Another solution may be to give to customers low-level system access, so that the customers can implement their own trusted computing mechanisms; this would alleviate some of the pressure on the provider to provide secure infrastructure.

The ways in which cloud solutions can be contrasted to traditional data center services were discussed, and this material was similar to that in the other two presentations. Of course privacy was raised as a central concern here too, and it was made clear that better encryption and compliance mechanisms will need to be developed and deployed.

The speaker concluded with a presentation of the TClouds¹ project, which deals with privacy and resilience for Internet-scale trustworthy infrastructures. The most relevant activity in the project dealing with trustworthy clouds is Activity 3, which deals with end-user application scenarios such as home health care monitoring (issues here include privacy and resilience) and capacity planning for the smart grid.

Discussion session

A number of questions were raised on the first presentation including:

- Can the cloud be trusted?
 - The response was 'both Yes and No'. For internal use, the answer is yes, as data is held and managed inside corporate systems; for external and customer use, at the moment, the answer is no.
- There is a need for *uniform* and consistent security and privacy regulation, but there is also a need for national laws and regulations that have to be equally respected. How do we balance the two?
 - The speaker explained that, in the context of the system designed for the French Ministry of Defense, the French MoD regulations override any EU regulations. It was also noted that for cloud based applications specifically for the French MoD, it was necessary for all data and servers to be physically located in France.
- It was pointed out that resiliency and duplication are among the greatest benefits of using cloud data centers. The question raised was - specifically with respect to the French situation/scenario, how do you keep data within the country, albeit in different

¹ <http://www.tclouds-project.eu/>

data centres, and also ensure they are not duplicated in countries where French law does not apply?

- The speaker responded that, as mentioned in the presentation, for specific applications developed for the French MoD, data is not permitted to be released outside the country. Sometimes the infrastructure used is temporary, but it has to stay in the country.
- If you are in Finland using services in Finland, it is possible that your IP packets will travel through Sweden. Clearly this can be a problem due to mismatches in law/regulation in these two (or any other two) countries. How does a cloud provider deal with this?
 - It was pointed out that it would become necessary to be able to guarantee end to end security.

A number of questions were raised regarding the second presentation:

- Are we to assume that the communication medium for clouds is de-facto the Internet?
 - The speaker answered yes, noting that it is a shared medium.
- What dedicated hardware might be required for the Future Internet's cloud based systems? Do we need a new processor design to cope with the real virtualisation that we are relying on in order to achieve separation, or is what is currently available sufficient? Do we need to look at the hardware processing design to be responsive to the new networking requirements?
 - A number of hardware companies in the audience responded that there is new hardware required, and some of these were already being tested in a number of R&D projects.
- Should be concerned when moving Virtual machines around and sending data between them, is it possible that the person who gets the data could be the adversary?
 - The response was yes, this was a possibility and needs to be safeguarded against.
- A comment was raised about when talking about virtualization, we often don't know what is "virtualized" and how the mechanisms are really used. When virtualising something, using several distinct virtualisation mechanisms, in order to secure several of these, there are several keys that are managed by different levels. Security is related to the articulation at the various mechanisms. Therefore, when talking about these virtualised levels, we run a risk of not comprehensively attacking the real security issues. This is an important challenge when dealing with the trust aspects.

A number of questions were raised on the third presentation including:

- Is there really a need for new applications when dealing with cloud computing, and what is the role of some of the projects dealing with the difference that cloud computing is supposed to make?

- the speaker responded that cloud computing does pose new challenges and that it will make a real difference to core security problems.
- How to migrate data from one cloud provider to another, and what implications does this have for standardization? This is one of the grand ideas behind open cloud standardization.
 - The view is that it is better to be involved in the standardization process than not to be.
- What is required for a Trusted cloud – to externally prove that the cloud is trustworthy?
 - a number of different trust levels were presented:
 - HIGH – having explicit, provable trust in provider
 - MEDIUM – having ability to see how provider is handling data
 - LOW - having the ability to actually control and monitor data and data flows.
- For online compliance testing and auditing, what is needed on the regulatory side or are we lacking the technology that provides the transparency?
 - Everyone needs to be accountable for every part of the transactions.
- Are there currently policy enforcement mechanisms specifically for clouds in place or is it still an active area of research?
 - The response was it is still an active area of research.
- The cloud is not transparent so how could it ever be trusted?
 - Trust will have to come out of trust models for reputation etc. Within the Future Internet, there is a need to add measurement around and inside clouds to get new variables to compute or estimate whether you can trust this cloud. A cloud is not an isolated bunker so you don't know when you enter the cloud. Therefore, security models must be very different for the cloud. Cloud is massive, with a lot of interactions, so we cannot know what is going on into a cloud and it is susceptible to interception and analysis. For example, there was a recent high profile example where spies were able to understand the heuristics of data by asking just a few basic questions.
- Do the models provide the means to determine when you cross into and out of the cloud zones?
 - An example of a toolset that does this is the **Tivoli** tool set.
 - Asked whether this can protect a private cloud, the difficult process of mapping between virtual layers and physical environments was described and some of the tools can apparently deal with this.

Links/additional info

The full set of slides will be available shortly at both the FIA Ghent official web site:

<http://fi-ghent.fi-week.eu/program/>

and the Trust and Security FIA wiki:

http://security.future-internet.eu/index.php/FIA_Ghent