

The Christian Doppler Laboratory for Client-Centric Cloud Computing

Application-Oriented Fundamental Research

Klaus-Dieter Schewe, Károly Bósa, Harald Lampesberger, Ji
Ma, **Boris Vleju**

The Christian Doppler Laboratory for Client-Centric Cloud Computing

June 7, 2011

- 1 About CDCC
- 2 Client Needs
- 3 Security and Privacy

The Christian Doppler Laboratory for Client-Centric Cloud Computing

- German Name:
 - Christian Doppler Labor für klientenorientiertes Cloud Computing
- Responsible Representative
 - Professor Dr. rer.nat.habil. Klaus-Dieter Schewe
 - Honorary Professor at the Johannes Kepler Universität Linz
 - Scientific Director of the Software Competence Center Hagenberg



Christian Doppler Research Association²

- Aims at promoting development in the areas of natural sciences, technology and economy
- Enables talented scientists in renowned research centers to achieve high-quality research and knowledge transfer
- Named after the Austrian physicist and mathematician, Christian Andreas Doppler

¹<http://www.jku.at>

²<http://www.cdg.ac.at>

Christian Doppler Research Association²

- Aims at promoting development in the areas of natural sciences, technology and economy
- Enables talented scientists in renowned research centers to achieve high-quality research and knowledge transfer
- Named after the Austrian physicist and mathematician, Christian Andreas Doppler
- The CD labs are established in universities or non-university research institutions for a maximum of seven years
- The CDCC is established within the Johannes Kepler Universität Linz ¹

¹<http://www.jku.at>

²<http://www.cdg.ac.at>

Close Scientific Collaboration

- **FAW** - Research Institute for Application-Oriented Knowledge Processing
- **SCCH** - Software Competence Center Hagenberg
- **RISC** - Research Institute for Symbolic Computation
- **FHH** - Upper Austria University of Applied Sciences Hagenberg

Industrial Partners

- **SecureGUARD GmbH**
 - Offers a unique portfolio of Internet security appliances for enterprises of all sizes
 - Plans to add unique, cloud computing related security features to their appliances



Industrial Partners

- **SecureGUARD GmbH**
 - Offers a unique portfolio of Internet security appliances for enterprises of all sizes
 - Plans to add unique, cloud computing related security features to their appliances
- **CloudGUARD GmbH**
 - Develops cloud specific security software at the point of the cloud service consumer
 - Plans to integrate academic research in their software product to give them a USP in their market area



Industrial Partners

- **SecureGUARD GmbH**
 - Offers a unique portfolio of Internet security appliances for enterprises of all sizes
 - Plans to add unique, cloud computing related security features to their appliances
- **CloudGUARD GmbH**
 - Develops cloud specific security software at the point of the cloud service consumer
 - Plans to integrate academic research in their software product to give them a USP in their market area
- **Quanmax**
 - One of the biggest computer manufacturers and Notebook pioneers in Austria
 - Plans new class of cloud-enabled devices which will provide a seamless, secure integration of cloud services



Goals

- Address primarily the research problems associated with the *client side* of cloud computing.

Goals

- Address primarily the research problems associated with the *client side* of cloud computing.
- Key questions addressed:

Goals

- Address primarily the research problems associated with the *client side* of cloud computing.
- Key questions addressed:
 - What are the expectations and benefits for companies, in particular small and medium enterprises, in cloud computing?

Goals

- Address primarily the research problems associated with the *client side* of cloud computing.
- Key questions addressed:
 - What are the expectations and benefits for companies, in particular small and medium enterprises, in cloud computing?
 - What are the security and privacy hazards (loss of control, data leaks, etc.) for clients and how can they be addressed to gain trust in cloud computing?

Goals

- Address primarily the research problems associated with the *client side* of cloud computing.
- Key questions addressed:
 - What are the expectations and benefits for companies, in particular small and medium enterprises, in cloud computing?
 - What are the security and privacy hazards (loss of control, data leaks, etc.) for clients and how can they be addressed to gain trust in cloud computing?
 - What flexibility can a client expect when joining, leaving or moving to/from clouds?



Planned Research

- Research program of the CDCC comprises two modules:
 - *Client Needs*
 - Address the clients' needs with respect to service mediation, adaptivity, transparency, client management, and all contractual problems between service providers and users associated with cloud computing.

Planned Research

- Research program of the CDCC comprises two modules:
 - *Client Needs*
 - Address the clients' needs with respect to service mediation, adaptivity, transparency, client management, and all contractual problems between service providers and users associated with cloud computing.
 - *Security and Privacy*
 - Most of the research that has been done so far focuses on the protection of the service providers
 - Client-related security aspects do not receive much attention
 - We move security problems on the client side into the focus of our research



Client Needs

- We identify research topics around adaptivity and transparency

Client Needs

- We identify research topics around adaptivity and transparency
- What do clients expect from cloud servers to satisfy their preferences, their used devices, and how can interoperability between clients be supported by clouds?



Client Needs

- We identify research topics around adaptivity and transparency
- What do clients expect from cloud servers to satisfy their preferences, their used devices, and how can interoperability between clients be supported by clouds?
- We also address:



Client Needs

- We identify research topics around adaptivity and transparency
- What do clients expect from cloud servers to satisfy their preferences, their used devices, and how can interoperability between clients be supported by clouds?
- We also address:
 - The evolution of cloud services in accordance with the development of the web



Client Needs

- We identify research topics around adaptivity and transparency
- What do clients expect from cloud servers to satisfy their preferences, their used devices, and how can interoperability between clients be supported by clouds?
- We also address:
 - The evolution of cloud services in accordance with the development of the web
 - The problem of services that result from integrating services and mediating such service operations



Client Needs

- We identify research topics around adaptivity and transparency
- What do clients expect from cloud servers to satisfy their preferences, their used devices, and how can interoperability between clients be supported by clouds?
- We also address:
 - The evolution of cloud services in accordance with the development of the web
 - The problem of services that result from integrating services and mediating such service operations
 - Non-functional business aspects associated with cloud computing



Adaptivity to Clients and Devices

- The property of a system to adapt itself to different contexts

Adaptivity to Clients and Devices

- The property of a system to adapt itself to different contexts
- We concentrate on research aiming at adaptivity:

Adaptivity to Clients and Devices

- The property of a system to adapt itself to different contexts
- We concentrate on research aiming at adaptivity:
 - To preferences of clients
 - We also want to investigate, which options should be made available for clients to express preferences



Adaptivity to Clients and Devices

- The property of a system to adapt itself to different contexts
- We concentrate on research aiming at adaptivity:
 - To preferences of clients
 - We also want to investigate, which options should be made available for clients to express preferences
 - To restrictions arising from channels



Adaptivity to Clients and Devices

- The property of a system to adapt itself to different contexts
- We concentrate on research aiming at adaptivity:
 - To preferences of clients
 - We also want to investigate, which options should be made available for clients to express preferences
 - To restrictions arising from channels
 - To specific requirements for end-devices (such as mobile devices)



Transparent Services

- The Cloud scenario emphasizes relationships between service providers and service seekers
 - Many-to-many relationship

Transparent Services

- The Cloud scenario emphasizes relationships between service providers and service seekers
 - Many-to-many relationship
- We want to enable client-to-client interaction in an almost direct way
 - The involvement of services is transparent to the users
 - *No traces of the client activity are left on the cloud server*



Transparent Services

- The Cloud scenario emphasizes relationships between service providers and service seekers
 - Many-to-many relationship
- We want to enable client-to-client interaction in an almost direct way
 - The involvement of services is transparent to the users
 - *No traces of the client activity are left on the cloud server*
- Possible applications



Transparent Services

- The Cloud scenario emphasizes relationships between service providers and service seekers
 - Many-to-many relationship
- We want to enable client-to-client interaction in an almost direct way
 - The involvement of services is transparent to the users
 - *No traces of the client activity are left on the cloud server*
- Possible applications
 - Transparent use of switching services
 - Clients communicate with each other
 - The cloud plays the role of switch data from one client to another



Transparent Services

- The Cloud scenario emphasizes relationships between service providers and service seekers
 - Many-to-many relationship
- We want to enable client-to-client interaction in an almost direct way
 - The involvement of services is transparent to the users
 - No traces of the client activity are left on the cloud server
- Possible applications
 - Transparent use of switching services
 - Clients communicate with each other
 - The cloud plays the role of switch data from one client to another
 - When execution of composed services requires the storage of intermediate result at a third-party cloud
 - The cloud provides storage space for the exclusive and temporary access by a composed service
 - No trace should be left after completion

Web 2.0 and Web 3.0 Services

- Commonly used buzzwords associated with particular offers such as YouTube, Facebook, MySpace, eBay, etc.
 - Hardly ever with a precise characterization what these developments of the world-wide web stand for

Web 2.0 and Web 3.0 Services

- Commonly used buzzwords associated with particular offers such as YouTube, Facebook, MySpace, eBay, etc.
 - Hardly ever with a precise characterization what these developments of the world-wide web stand for
- From what we see so far, the main research challenge is:



Web 2.0 and Web 3.0 Services

- Commonly used buzzwords associated with particular offers such as YouTube, Facebook, MySpace, eBay, etc.
 - Hardly ever with a precise characterization what these developments of the world-wide web stand for
- From what we see so far, the main research challenge is:
 - Collaborative service-oriented applications
 - Comprises cooperation, communication and coordination
 - We face the problem of a group of actors solving a problem by using services
 - Can be tackled by bringing in a second level of mediation in which slots are first filled in by actors in the group
 - Our intention is to study conditions for group mediation in depth and to extend the theory of mediators



Contracting as a Service

- The setup of contracts is considered an activity that involves both a service provider and a service user
 - Advisable to bundle contracting activities as a separate service to be offered by a cloud

Contracting as a Service

- The setup of contracts is considered an activity that involves both a service provider and a service user
 - Advisable to bundle contracting activities as a separate service to be offered by a cloud
- We intend to:

Contracting as a Service

- The setup of contracts is considered an activity that involves both a service provider and a service user
 - Advisable to bundle contracting activities as a separate service to be offered by a cloud
- We intend to:
 - Investigate the specification and semantic description of such contracting services

Contracting as a Service

- The setup of contracts is considered an activity that involves both a service provider and a service user
 - Advisable to bundle contracting activities as a separate service to be offered by a cloud
- We intend to:
 - Investigate the specification and semantic description of such contracting services
 - Develop algorithms for contract integration

Contracting as a Service

- The setup of contracts is considered an activity that involves both a service provider and a service user
 - Advisable to bundle contracting activities as a separate service to be offered by a cloud
- We intend to:
 - Investigate the specification and semantic description of such contracting services
 - Develop algorithms for contract integration
 - Develop methods that generate a resulting SLA out of the SLAs of the services with weights associated to services by the services users



Security and Privacy

- Our goal is:

Security and Privacy

- Our goal is:
 - To ensure formal properties that can increase trustworthiness
 - To have a clear list of security hazards for clients and formal means how to handle these hazards

Security and Privacy

- Our goal is:
 - To ensure formal properties that can increase trustworthiness
 - To have a clear list of security hazards for clients and formal means how to handle these hazards
- We consider the basic problem of message encryption as solved
 - This does not imply that all security and privacy problems can be treated as being solved as well



Security and Privacy

- Our goal is:
 - To ensure formal properties that can increase trustworthiness
 - To have a clear list of security hazards for clients and formal means how to handle these hazards
- We consider the basic problem of message encryption as solved
 - This does not imply that all security and privacy problems can be treated as being solved as well
- We will highlight problems
 - With access control
 - Preservation of secrecy and anonymity
 - With trustworthiness of clients
 - With varying group allocations and consequences for client credentials



Management of Access Rights

- We intend to investigate two research problems:



Management of Access Rights

- We intend to investigate two research problems:
 - The checking of access rights
 - We intend to develop adequate methods
 - The problem is to keep track of dependencies between group rights and rights of group members



Management of Access Rights

- We intend to investigate two research problems:
 - The checking of access rights
 - We intend to develop adequate methods
 - The problem is to keep track of dependencies between group rights and rights of group members
 - Inferences on access rights
 - Ownership should imply access rights
 - Membership in a group should imply that access rights of the group also apply to its members
 - The right to execute a service operation should imply the right to execute the underlying view
 - The goal is to ensure that all implied access rights must be explicitly granted



Identity Management

- Our first task is to obtain a precise definition of identity
 - Starting from the attempt that an identity refers to an actor or group in a set of roles



Identity Management

- Our first task is to obtain a precise definition of identity
 - Starting from the attempt that an identity refers to an actor or group in a set of roles
- For security we plan to investigate:

Identity Management

- Our first task is to obtain a precise definition of identity
 - Starting from the attempt that an identity refers to an actor or group in a set of roles
- For security we plan to investigate:
 - Whether the collection of access rights/owned data/software permits activities that would normally require additional access rights
 - Should lead to the development of alert algorithms



Identity Management

- Our first task is to obtain a precise definition of identity
 - Starting from the attempt that an identity refers to an actor or group in a set of roles
- For security we plan to investigate:
 - Whether the collection of access rights/owned data/software permits activities that would normally require additional access rights
 - Should lead to the development of alert algorithms
 - Users may lose roles and the corresponding access rights
 - It may be necessary to delete data and software owned by an identity
 - Ownership changes to one of the groups the identity belonged to



Client Health Checking

- We intend to investigate potential attacks that may arise from granting access to clients

Client Health Checking

- We intend to investigate potential attacks that may arise from granting access to clients
- We want to:

Client Health Checking

- We intend to investigate potential attacks that may arise from granting access to clients
- We want to:
 - Discover what risks exist for a cloud and its users, if a client is vulnerable to attacks

Client Health Checking

- We intend to investigate potential attacks that may arise from granting access to clients
- We want to:
 - Discover what risks exist for a cloud and its users, if a client is vulnerable to attacks
 - Develop protocols to prevent potential attacks through client-side security gaps



Client Health Checking

- We intend to investigate potential attacks that may arise from granting access to clients
- We want to:
 - Discover what risks exist for a cloud and its users, if a client is vulnerable to attacks
 - Develop protocols to prevent potential attacks through client-side security gaps
 - Research the possibility of adaptive security on base of the result of the health check
 - Totally healthy client is allowed to perform all functionality
 - Other clients have limited access rights



Client Health Checking

- We intend to investigate potential attacks that may arise from granting access to clients
- We want to:
 - Discover what risks exist for a cloud and its users, if a client is vulnerable to attacks
 - Develop protocols to prevent potential attacks through client-side security gaps
 - Research the possibility of adaptive security on base of the result of the health check
 - Totally healthy client is allowed to perform all functionality
 - Other clients have limited access rights
 - Research the possibility that the health check is performed by an on premise device
 - Security policy never leaves the company
 - Will lead to a paradigm change since now the "client" is providing services for the cloud



Client Health Checking

- We intend to investigate potential attacks that may arise from granting access to clients
- We want to:
 - Discover what risks exist for a cloud and its users, if a client is vulnerable to attacks
 - Develop protocols to prevent potential attacks through client-side security gaps
 - Research the possibility of adaptive security on base of the result of the health check
 - Totally healthy client is allowed to perform all functionality
 - Other clients have limited access rights
 - Research the possibility that the health check is performed by an on premise device
 - Security policy never leaves the company
 - Will lead to a paradigm change since now the "client" is providing services for the cloud
 - Further extension of this thoughts will lead to "*Security as a Service*"



Protection of Secrets and Anonymity

- Aims at making data available only to those actors who are authorized to see the data while protecting their anonymity

Protection of Secrets and Anonymity

- Aims at making data available only to those actors who are authorized to see the data while protecting their anonymity
- We will pick up on the idea of specification of secrets
 - At which granularity level such secret specifications should be applied in the data model



Protection of Secrets and Anonymity

- Aims at making data available only to those actors who are authorized to see the data while protecting their anonymity
- We will pick up on the idea of specification of secrets
 - At which granularity level such secret specifications should be applied in the data model
- We have to be aware that secrets may nonetheless be discovered by means of inferences
 - Distinguish between exact detection of a secret, detection with a tolerable error, and detection with a high probability



Protection of Secrets and Anonymity

- Aims at making data available only to those actors who are authorized to see the data while protecting their anonymity
- We will pick up on the idea of specification of secrets
 - At which granularity level such secret specifications should be applied in the data model
- We have to be aware that secrets may nonetheless be discovered by means of inferences
 - Distinguish between exact detection of a secret, detection with a tolerable error, and detection with a high probability
- We will also investigate the alternatives of blocking certain queries, if the result could be used to discover secrets
 - Based on feasibility studies

Protection of Secrets and Anonymity

- Aims at making data available only to those actors who are authorized to see the data while protecting their anonymity
- We will pick up on the idea of specification of secrets
 - At which granularity level such secret specifications should be applied in the data model
- We have to be aware that secrets may nonetheless be discovered by means of inferences
 - Distinguish between exact detection of a secret, detection with a tolerable error, and detection with a high probability
- We will also investigate the alternatives of blocking certain queries, if the result could be used to discover secrets
 - Based on feasibility studies
- We also want to allow a customer to retrieve data without being able to see the actual query
 - We intend to study replication strategies and develop algorithms for query execution that preserve anonymity

Thank you

