Universität der Bundeswehr München

Gabi Dreo Rodosek, Mario Golling,
Wolfgang Hommel, Alexander Reinhold

Inter-Clouds: Einsatzmöglichkeiten und Anforderungen an die IT-Sicherheit

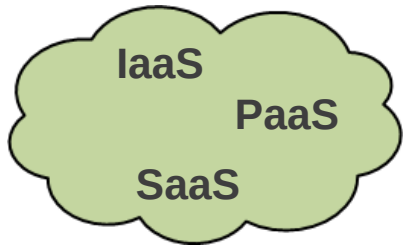
Regensburg, 22.05.2012

Cloud-Computing

der Bundeswehr Universität München

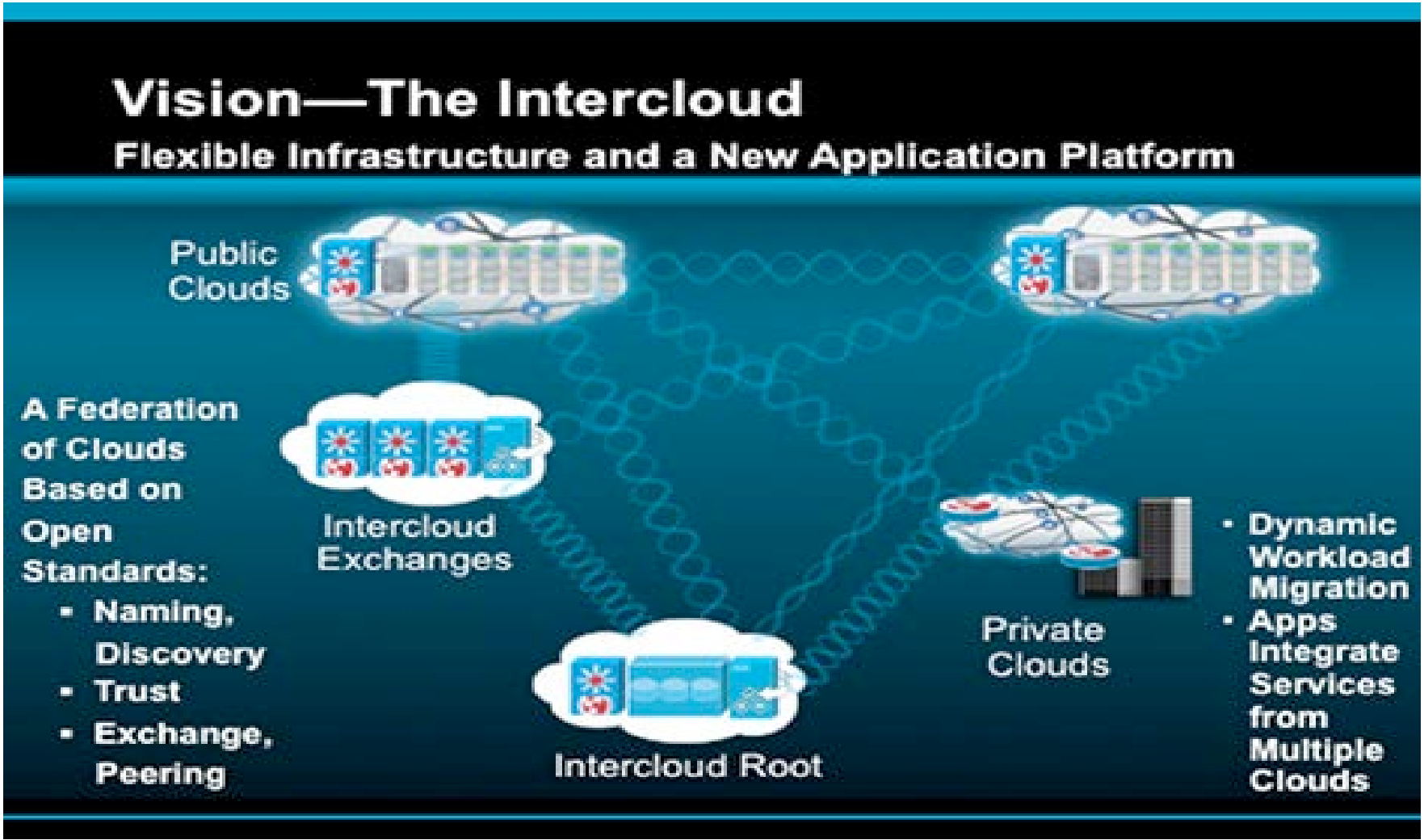
+ Flexibler Zugriff auf Ressourcen
+ Schnelle Entwicklung neuartiger, kundenspezifischer Dienste, Anwendungen und Lösungen

– Mangelende IT-Sicherheit
– Beachtung rechtlicher Bestimmungen (BDSG)



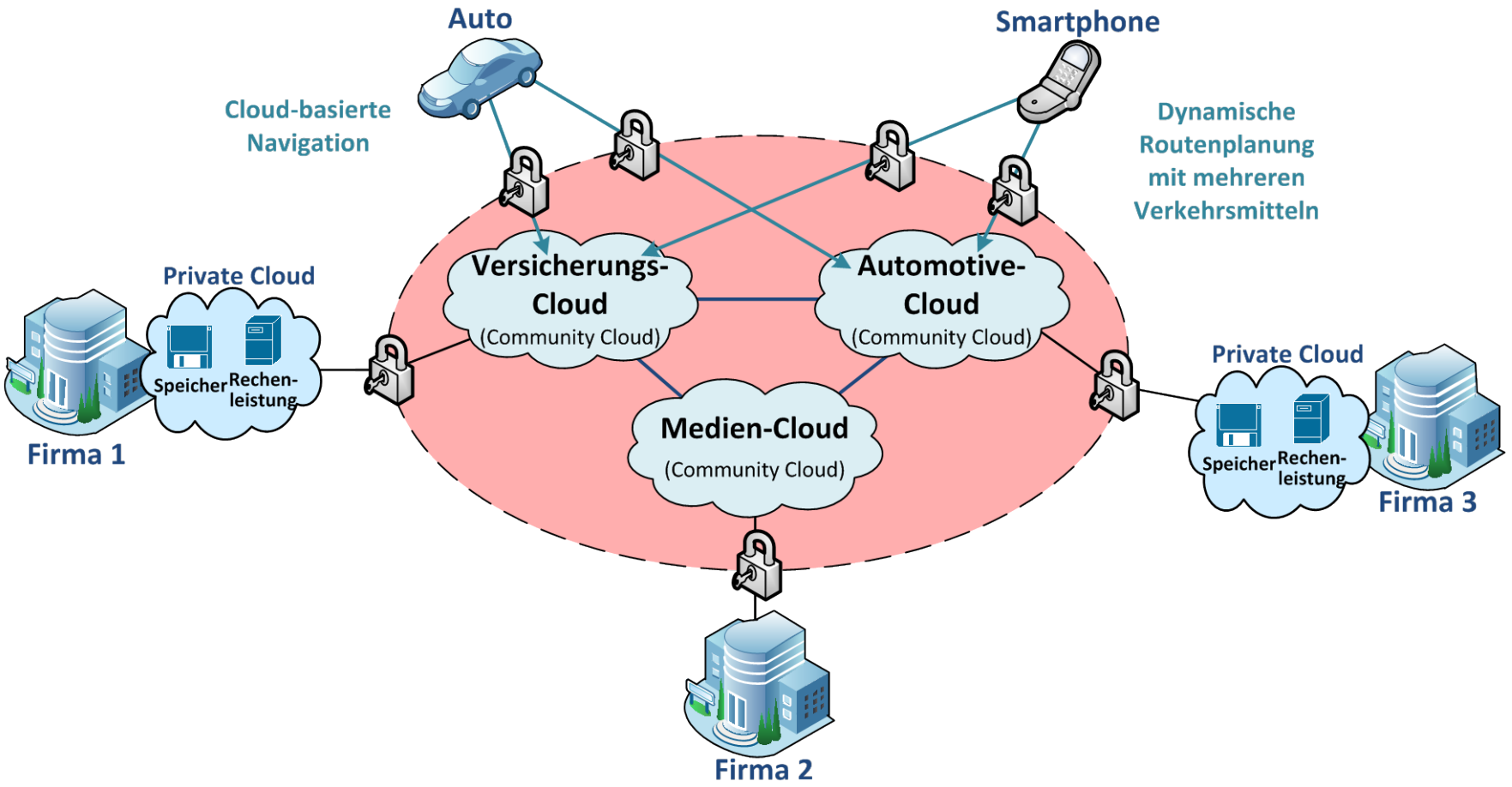
Von Clouds zu Inter-Clouds (1)

Unterschiedliche Ansätze z.B. von Cisco



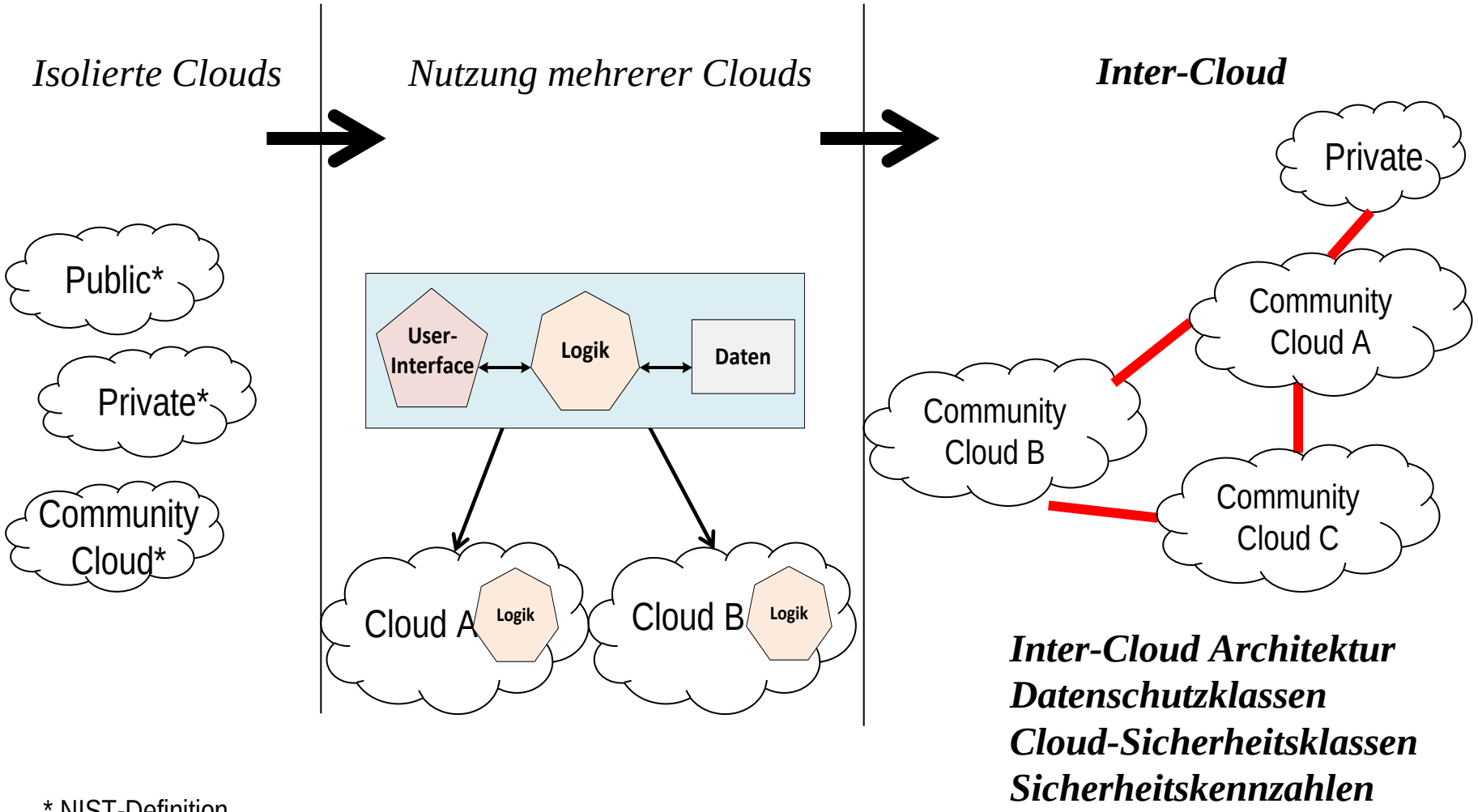
Von Clouds zu Inter-Clouds (2)

der Bundeswehr Universität München



Zur Sicheren Inter-Cloud

der Bundeswehr Universität München

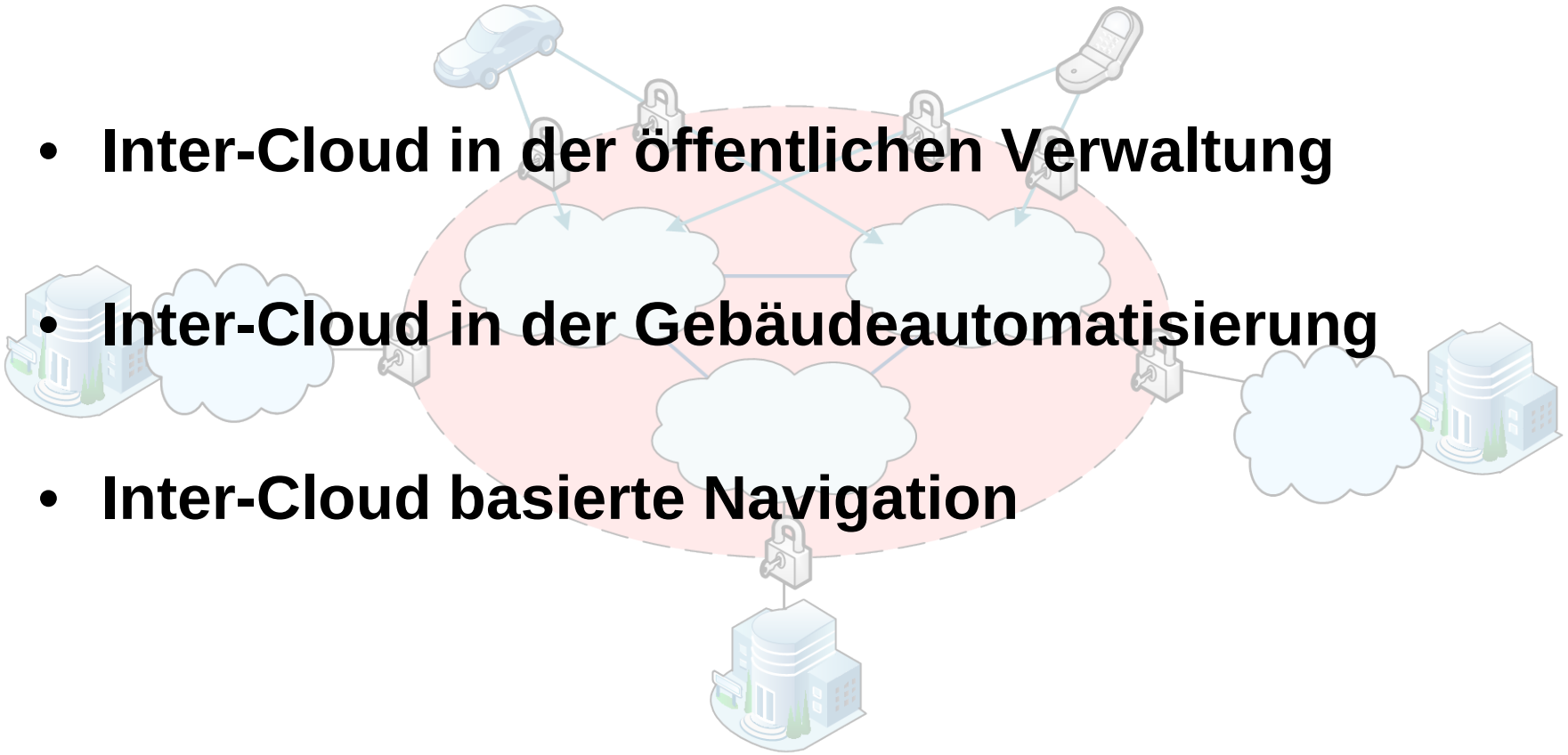


Inter-Cloud Architektur
Datenschutzklassen
Cloud-Sicherheitsklassen
Sicherheitskennzahlen

* NIST-Definition

Anwendungsbeispiele

der Bundeswehr Universität München



- Inter-Cloud in der öffentlichen Verwaltung
- Inter-Cloud in der Gebäudeautomatisierung
- Inter-Cloud basierte Navigation

Steuerung des Verkehrs in Großstädten

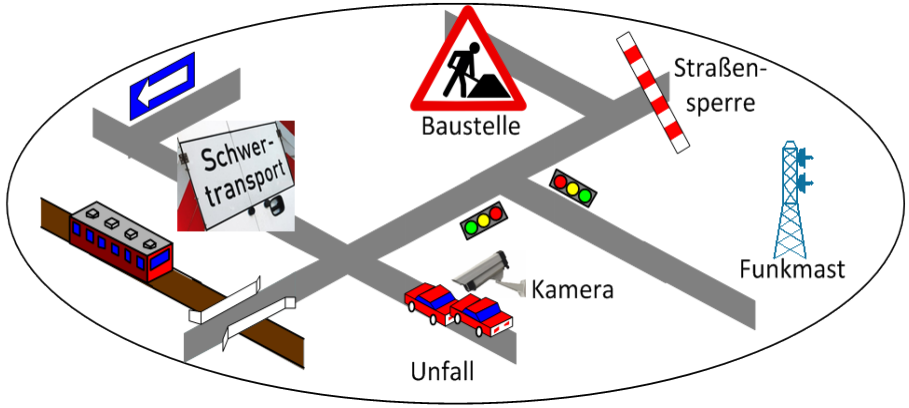
der Bundeswehr Universität München

- Navigation nur auf Basis lokaler Daten (auf Navi) und TMC
- Verkehrsflusssteuerung sehr limitiert

Lokale Routenberechnung

TOMTOM

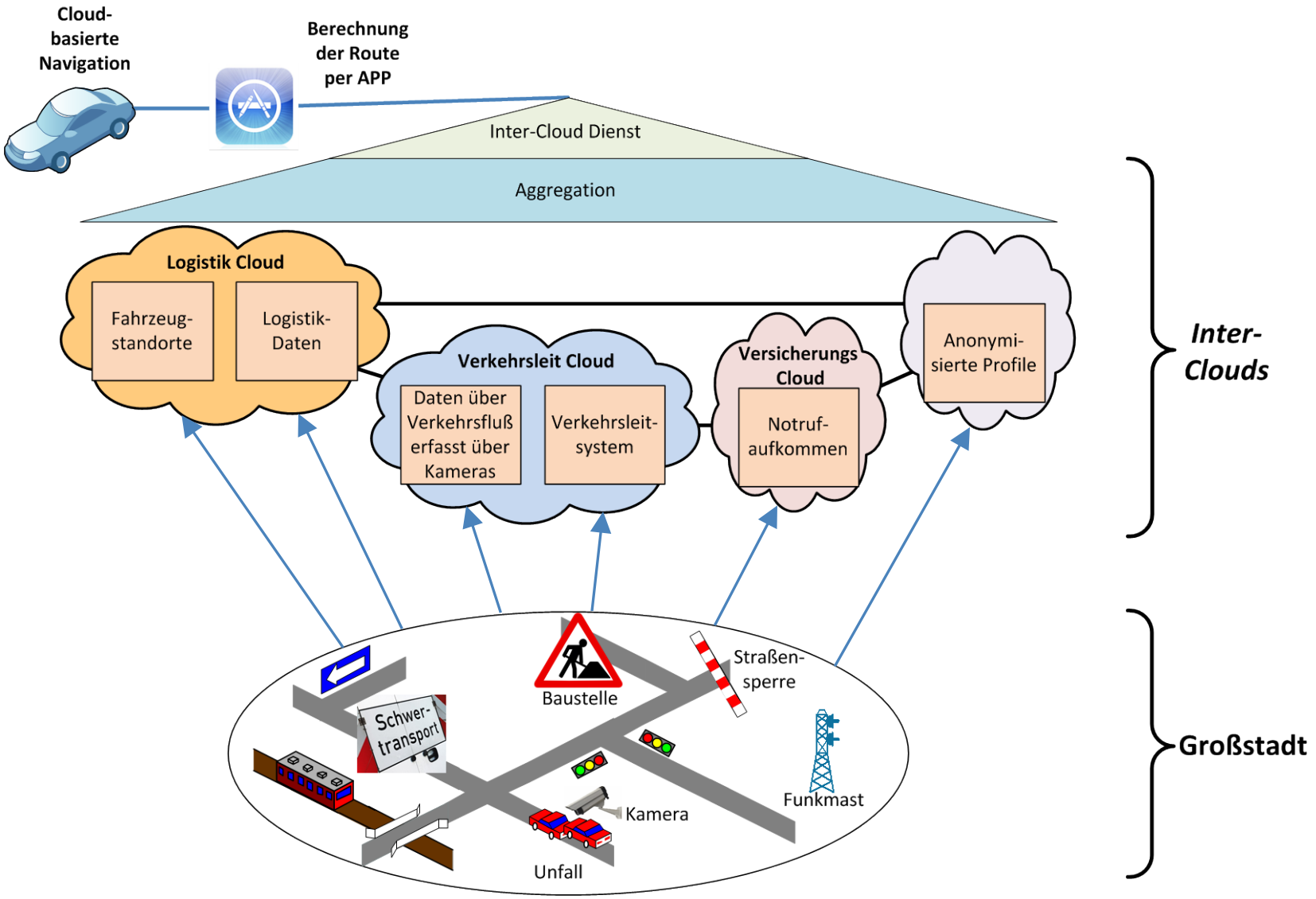
TMC TRAFFIC MESSAGE CHANNEL



Stadt München

Inter-Cloud basierte Navigation

der Bundeswehr Universität München



Anforderungsanalyse (1)

Universität der Bundeswehr München

Herausforderung	Lösungsmöglichkeit
• Missbräuchliche Erstellung personifizierte Bewegungs- und Nutzungsprofile durch Datenkumulation	⇒ Weitestgehende Verarbeitung anonymisierter bzw. pseudonymisierter Daten
• Derzeit mangelnde Datensicherheit in Inter-Cloud-Umgebungen	⇒ Datenschutzklassen legen ausgeprägte Sicherheitsmechanismen für die Datenspeicherung und den -transport fest
• Verbund mehrerer Clouds setzt verifizierbares Vertrauen voraus	⇒ Trust Management System auf Basis einer Klassifizierung und Reputation

Anforderungsanalyse (2)

Universität der Bundeswehr München

Herausforderung	Lösungsmöglichkeit
• Organisationsübergreifende Authentifizierungs- und Autorisierungsinfrastruktur	⇒ Föderiertes Identitäts-management
• Neue Angriffsvektoren und Missbrauchsmöglichkeiten	⇒ Entwicklung / Portierung entsprechender Erkennungsverfahren

⇒ Auditier- und Verifizierbarkeit, um Vertauen gewährleisten zu können

Gegenüberstellung

der Bundeswehr Universität München

	Verarbeitung personenbezogener Daten	Erstellen von Nutzungsprofilen	NDAs bei Business-Cloud-Anwendungen	Konform zum BDSG	Anonymisierte Datenverarbeitung	Schutzklassen für Daten	Nutzung standardisierter Protokolle	Authentifizierungs- und Autorisierungskonzepte	Usability berücksichtigt, u.a. GUIs und Single Sign-On	Trust Level Management	Einfache Integration neuer Cloud-Dienste	Spezifizierte Prozesse u.a. für Risikomanagement	Sicherheitskennzahlen	Betriebswirtschaftliche und rechtliche Anforderungen	Policy Enforcement, z.B. der Datenklassifizierung	Cloud-spezifische Angriffserkennung	Demonstrator und praktische Bewertung	Zusammenarbeit mit Standardisierungsgremien	
CloudCycle	x		x	x				x		x	*				x				* Security-Plugins
Value4Cloud								x		x	x			x			x		
Sealed Cloud				x			x	x		x			x	x	x		x	x	
Mimo Secco							x	x		x							x		
SkIDentity	x			x				x						x	x		x		
MIA											x			x	x				
Cloud4E											x			x					
Peer Energy Cloud		x			*														* außerhalb der Cloud
Sensor Cloud		x			*														* außerhalb der Cloud
CollabCloud	x										x			x					
Sec2	x						x	x									x		
Berlin City Cloud	x													x			x		
goBerlin	x										x			x			x		
Frankfurt Cloud							x				x				x				
Eurocloud			x	x			x					x		x	x			x	
mOSAIC							x				x								
BonFIRE							x				x								
VENUS-C											x								
StratusLab							x	x			*								* nur Ressourcen-Integration
Deutsche Wolke				x			x	x											

Fragestellungen (1)

1. Analyse der **Anforderungen** aus Sicht der Anwender (Allianz, BMW, LHM, Bosch, ...
2. Spezifikation einer **Sicherheitstaxonomie** (Datenschutzklassen, Cloud-Sicherheitsklassen)
3. Spezifikation **einer IT-Sicherheitsarchitektur** für Inter-Clouds, um u.a. folgende Fragestellungen zu lösen
    a) Spezifikation eines Protokolls zu sicheren Inter-Cloud Kommunikation
    b) Spezifikation eines Inter-Cloud Identity Managements

Fragestellungen (2)

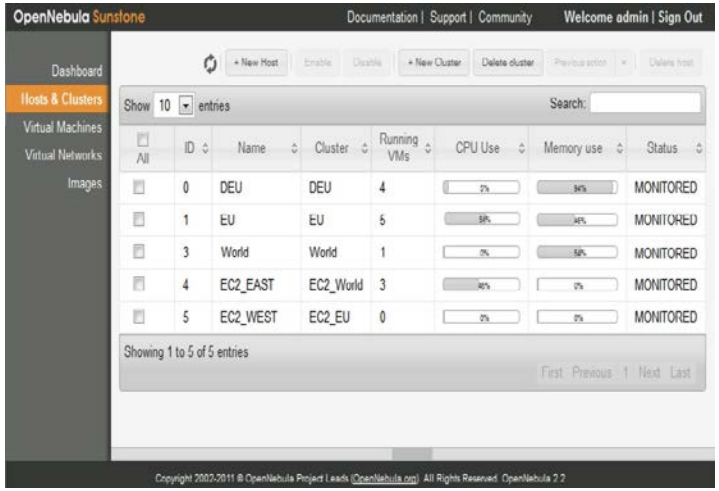
Universität der Bundeswehr München

3. Spezifikation von **Korrelationsverfahren** für die Verdichtung von Security-Events, Generierung von Sicherheitskennzahlen
4. Konzeption eines Cloud-weiten **Trust-Level-Managements**, u.a. mit der Entwicklung von Modellen für Vertrauenswerte und deren Berechnung, Entwicklung und Umsetzung von Policies (Richtlinien)
5. Konzeption einer Architektur zur **Angriffsdetektion** in Inter-Cloud („IDS für Inter-Cloud“) mit u.a. Schnittstellen zur Verwaltung des Regelwerks für verhaltensbasierte Detektion

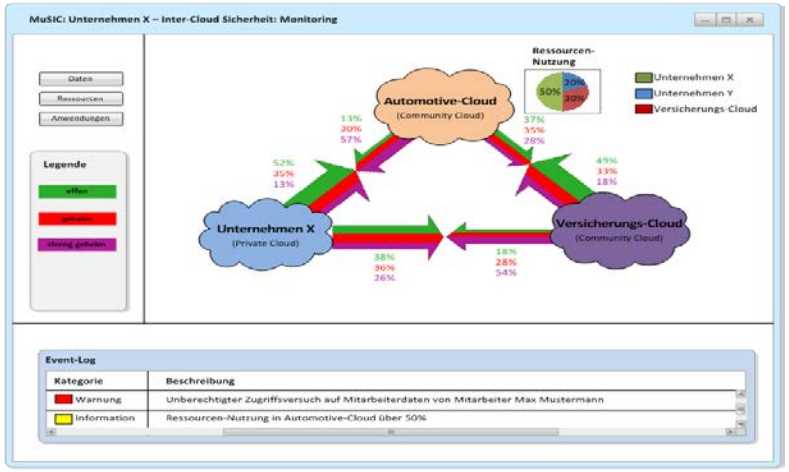
Innovation

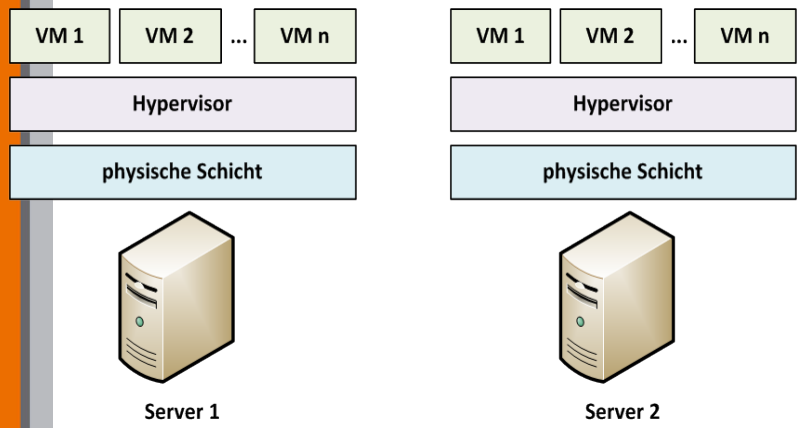
der Bundeswehr Universität München

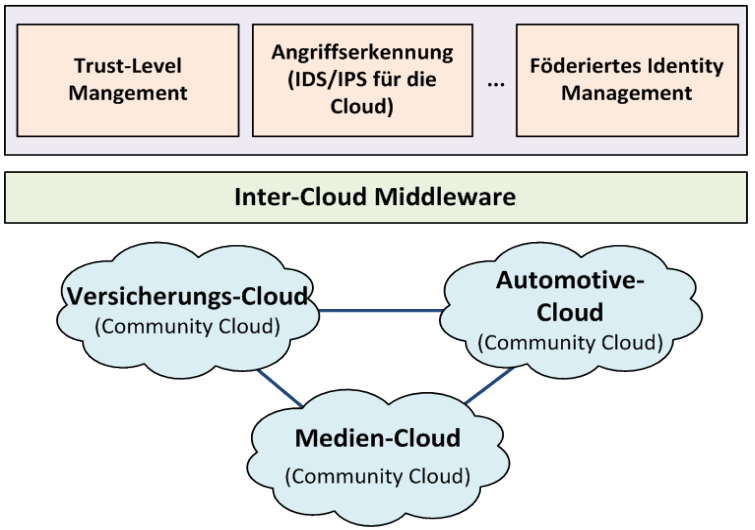
Stand der Technik



MuSIC







Vielen Dank für Ihre Aufmerksamkeit!

Prof. Dr. Gabi Dreo Rodosek
Lehrstuhl für Kommunikationssysteme und Internet-Dienste
Werner-Heisenberg-Weg 39
85577 Neubiberg

gabi.dreo@unibw.de