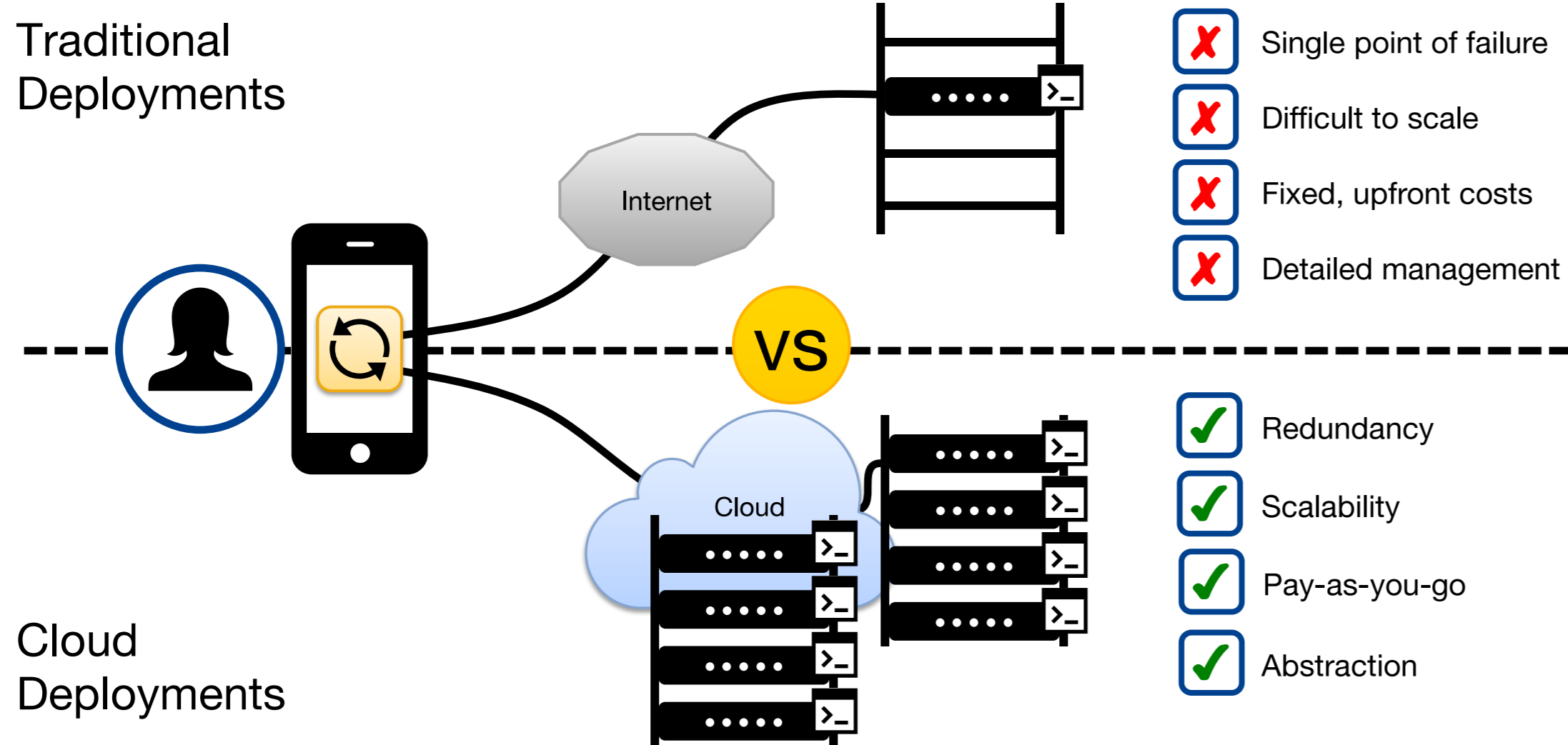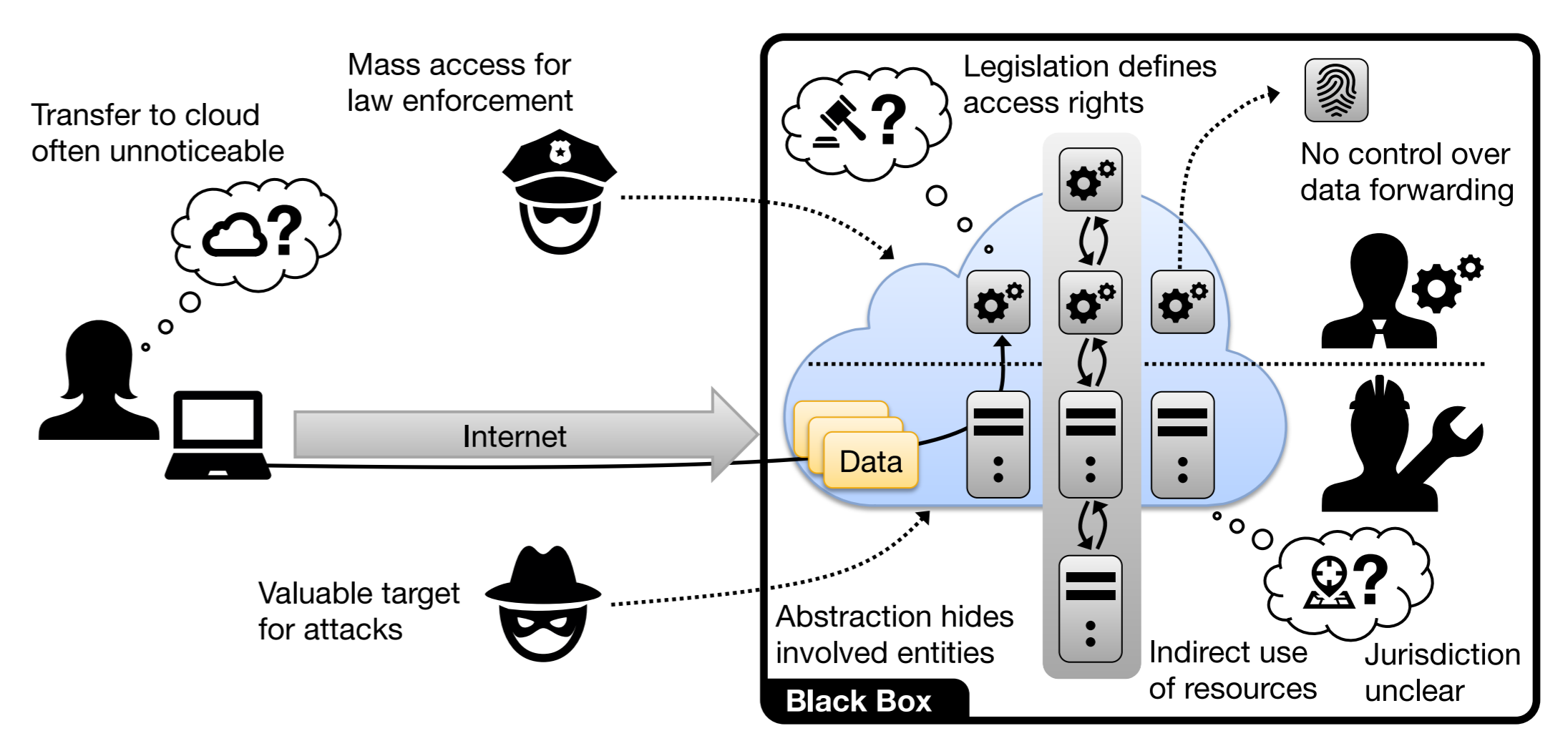# Accounting for Privacy in the Cloud Computing Landscape

Motivation and Problem Analysis

Benefits of Cloud Computing

Traditional Deployments

Internet

Cloud Deployments

Internet

Cloud

VS

- ✗ Single point of failure
- ✗ Difficult to scale
- ✗ Fixed, upfront costs
- ✗ Detailed management
- ✓ Redundancy
- ✓ Scalability
- ✓ Pay-as-you-go
- ✓ Abstraction

Core Problems for Privacy in Cloud Computing

Transfer to cloud often unnoticeable

Mass access for law enforcement

Legislation defines access rights

No control over data forwarding

Internet

Data

Valuable target for attacks

Abstraction hides involved entities

Indirect use of resources
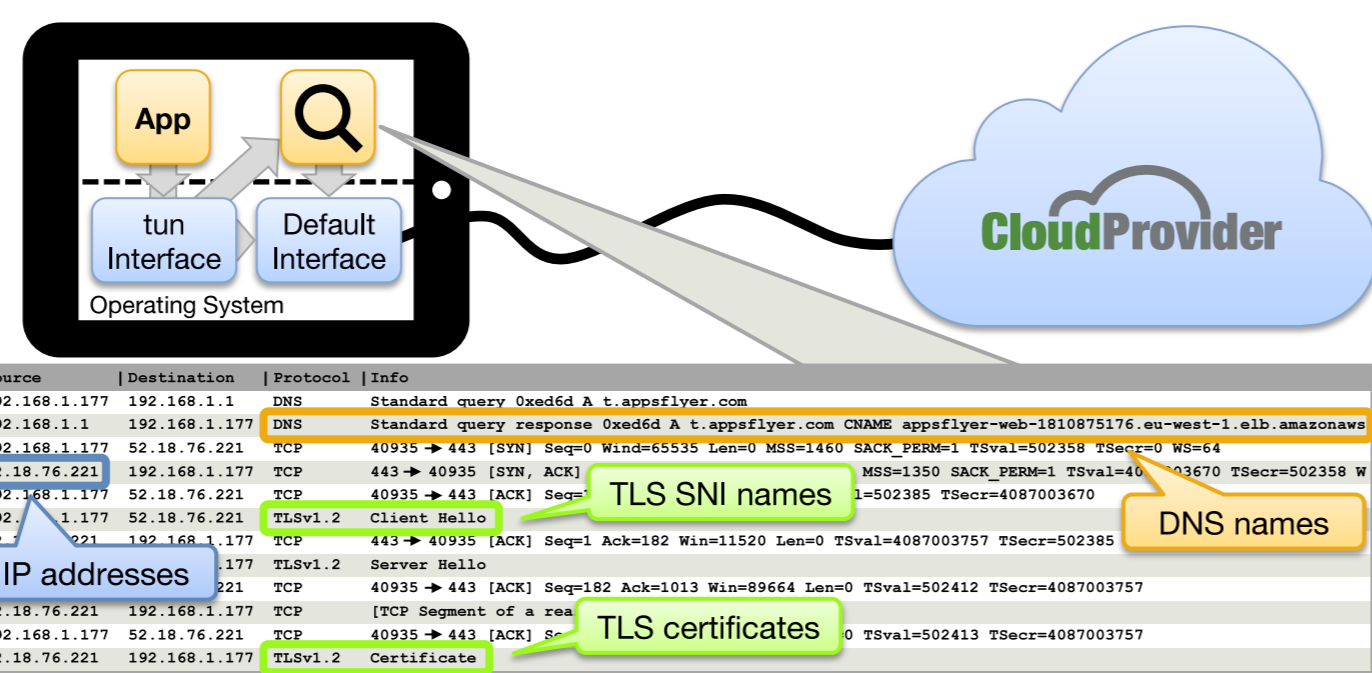
Jurisdiction unclear

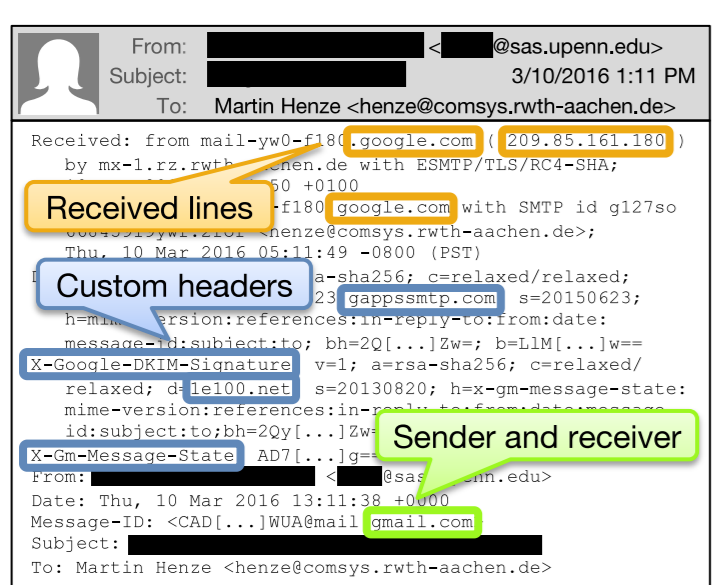Black Box

Approach and Contributions

Raising Awareness for Cloud Usage

- Mobile apps and email services heavily rely on cloud services
  - ‣ Users need to be aware of this cloud usage to assess and counter potential privacy risks
- Android app that detects cloud usage of apps
  - ‣ Covers 55 representative cloud services and infrastructures
  - ‣ Operates on unmodified Android
  - ‣ Detect communication with cloud services in network traffic
  - ‣ Evaluated in a user study and measurements of popular apps and mobile websites

App

tun Interface / Default Interface

Operating System

CloudProvider

TLS SNI names

DNS names

IP addresses

TLS certificates

COMSYS/CloudAnalyzer

- Similar approach for emails
  - ‣ Detects cloud usage based on information recorded in email headers
  - ‣ Used to assess the cloud utilization of email infrastructure (complete IPv4 space, 154M domain names)
  - ‣ Uncover the usage of cloud resources in 31M emails

Received lines

Custom headers

Sender and receiver

COMSYS/MailAnalyzer

Cloud Usage

- Contextualization
  - ‣ Users need assistance in objectifying statistics on their personal cloud usage
  - ‣ Allow users to anonymously compare their cloud usage against their peer group
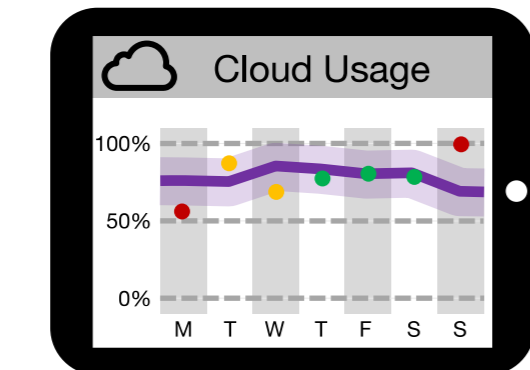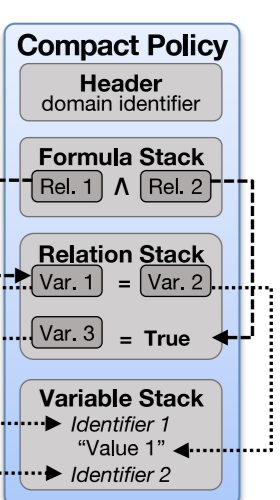
Data Handling Requirements-aware Cloud

- Clients have requirements how their data should be handled in the cloud
  - ‣ Triggered by intrinsic motivations or statutory regulations (e.g., data protection legislation)
- Support cloud providers to meet these requirements by annotating data
  - ‣ Enrich data with privacy policies specifying allowed data handling and secondary usage

Data Policy

- Compact privacy policy language for the machine-readable expression of clients' data handling requirements
  - ‣ Incorporate domain knowledge to achieve small policy sizes and efficient evaluation of resulting policies on the provider side
    - ‣ Per-data item polices let users stay in control over data in an increasingly interconnected world

Compact Policy
Header
domain identifier
Formula Stack
Rel. 1 | Rel. 2
Relation Stack
Var. 1 | Var. 2
Var. 3 = True
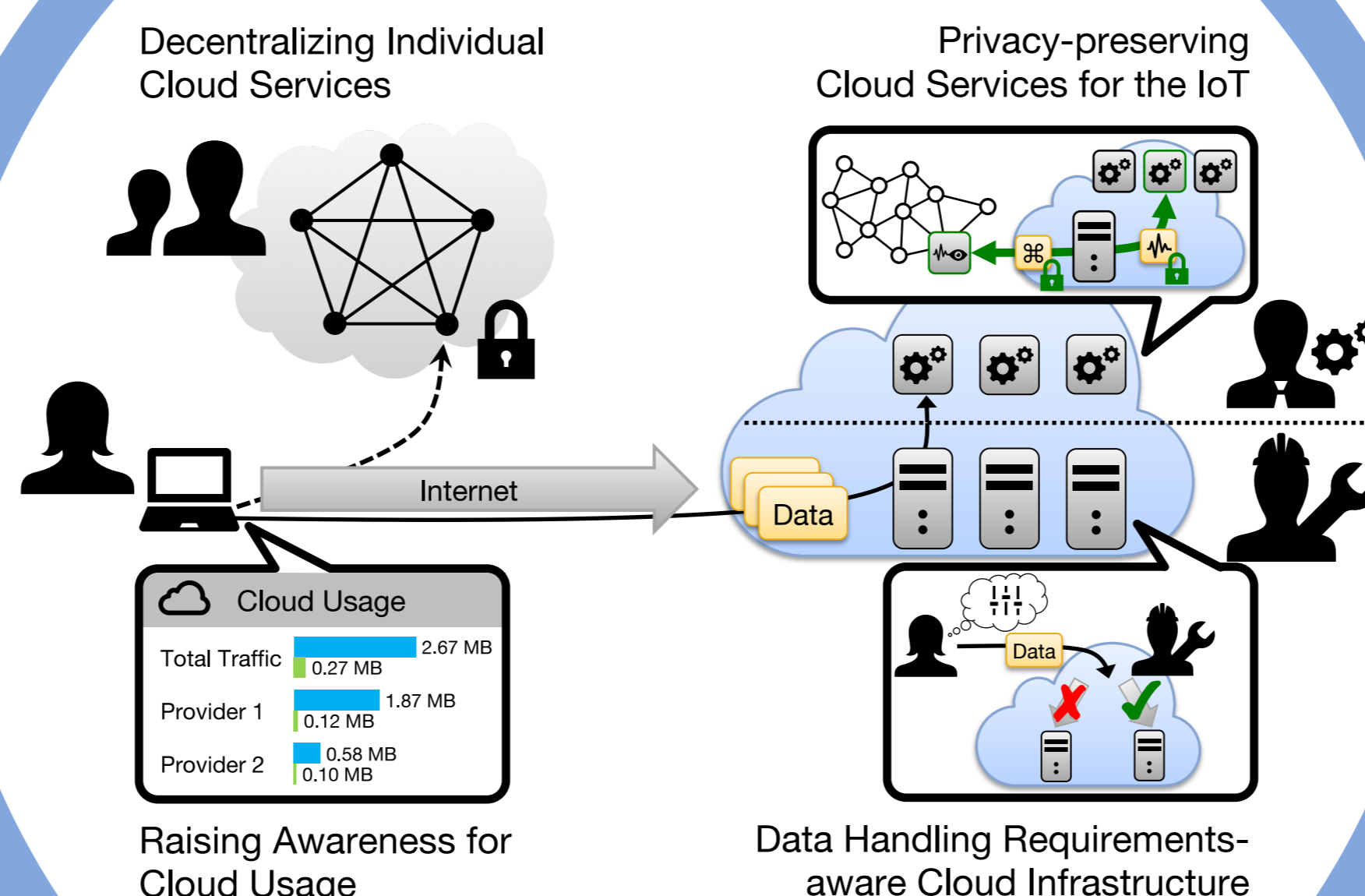Variable Stack
Identifier 1 "Value 1"
Identifier 2

COMSYS/CPPL

- Extending cloud storage systems with support for client's data handling requirements
  - ‣ Introduce indirection layer to only store data on policy compliant nodes
  - ‣ Proof-of-concept implementation on top of Cassandra database

H( )

COMSYS/Prada

Overview of Contributions

Decentralizing Individual Cloud Services

Privacy-preserving Cloud Services for the IoT

Internet

Data

Cloud Usage

Total Traffic	2.67 MB
	0.27 MB
Provider 1	1.87 MB
	0.12 MB
Provider 2	0.58 MB
	0.10 MB

Raising Awareness for Cloud Usage

Data Handling Requirements-aware Cloud Infrastructure

Addressing the core problems of cloud privacy is possible if the different actors cooperate!
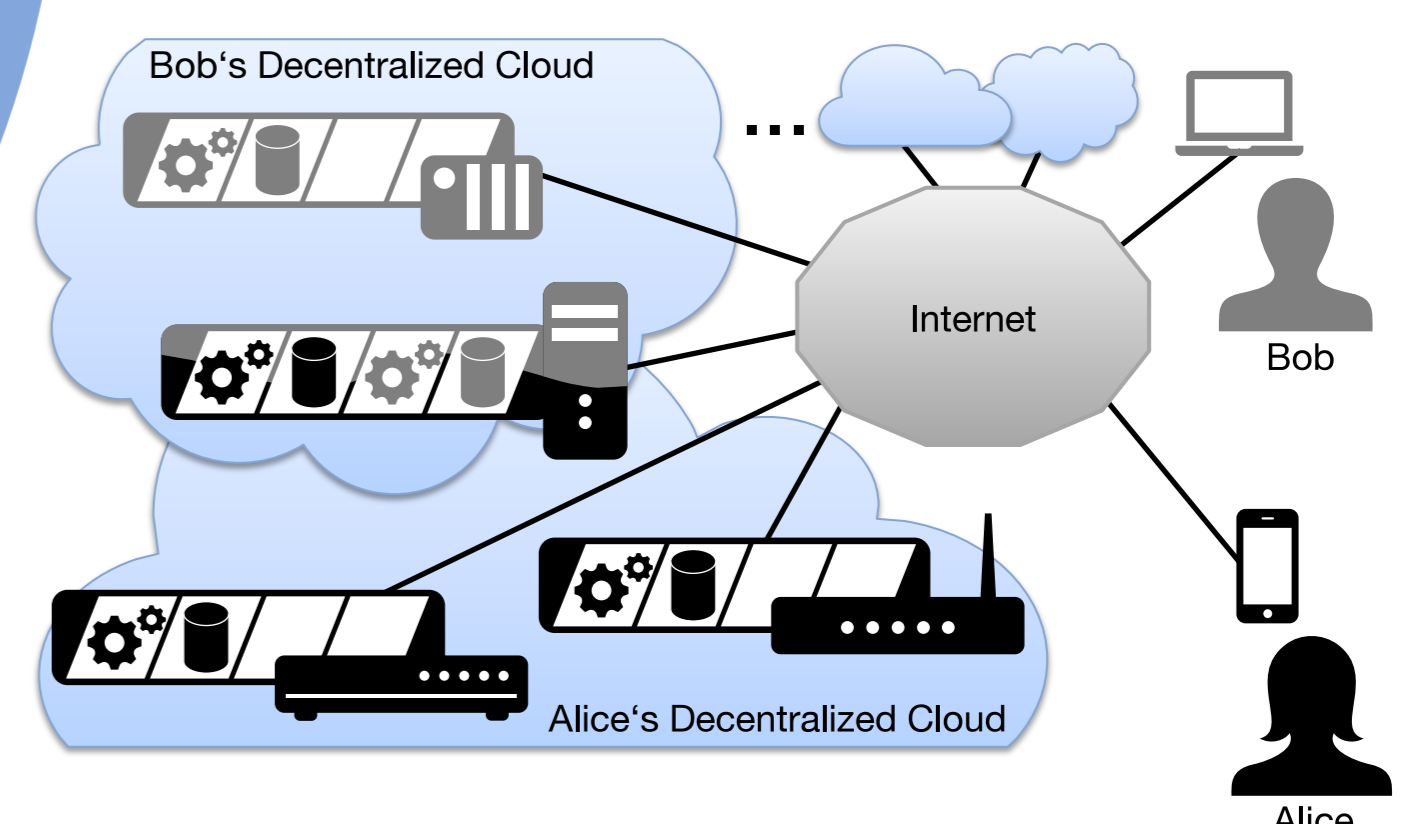
Privacy-preserving Services

- Developers require support in realizing privacy-preserving and secure cloud services
  - ‣ Often, domain specialists are no security experts
- Distributed architecture to configure, authorize and manage IoT devices across network borders
  - ‣ Instead of giving full control to the cloud, cloud is only used to securely realize a highly available and scalable message store
  - ‣ Only authorized parties can configure IoT devices
  - ‣ Malicious cloud providers cannot tamper with IoT configurations

D | GW

Append

Message Log

Verify

GW | D

Group Management

Log Trimming
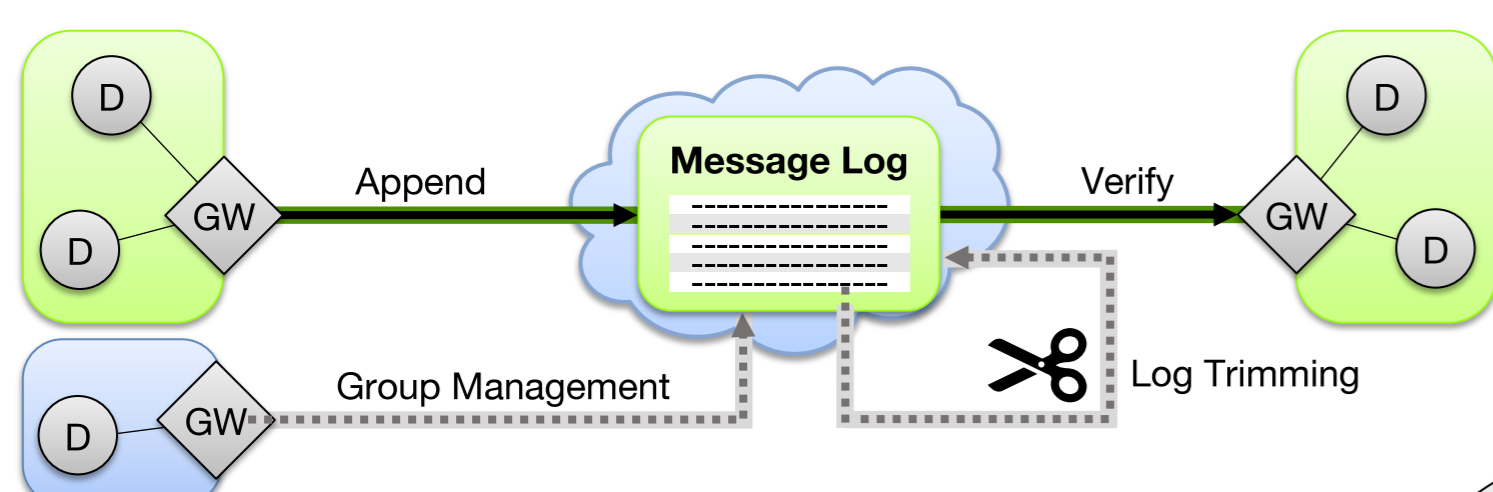
- Transparently accessing encrypted and integrity protected IoT data in the cloud
  - ‣ Security library for transparent access to protected IoT data stored in the cloud
  - ‣ Unburdens service developers from implementing security functionality
  - ‣ Build upon standardized approach to represent and protect IoT data
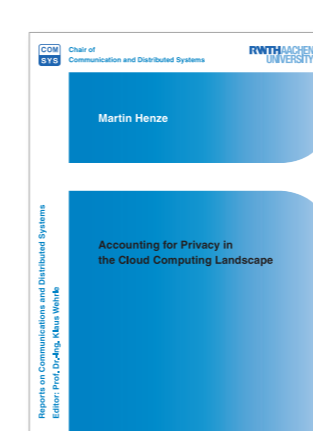 - ‣ Does not require any security expertise from cloud service developers

Service

Security Layer
abstraction of all security mechanisms
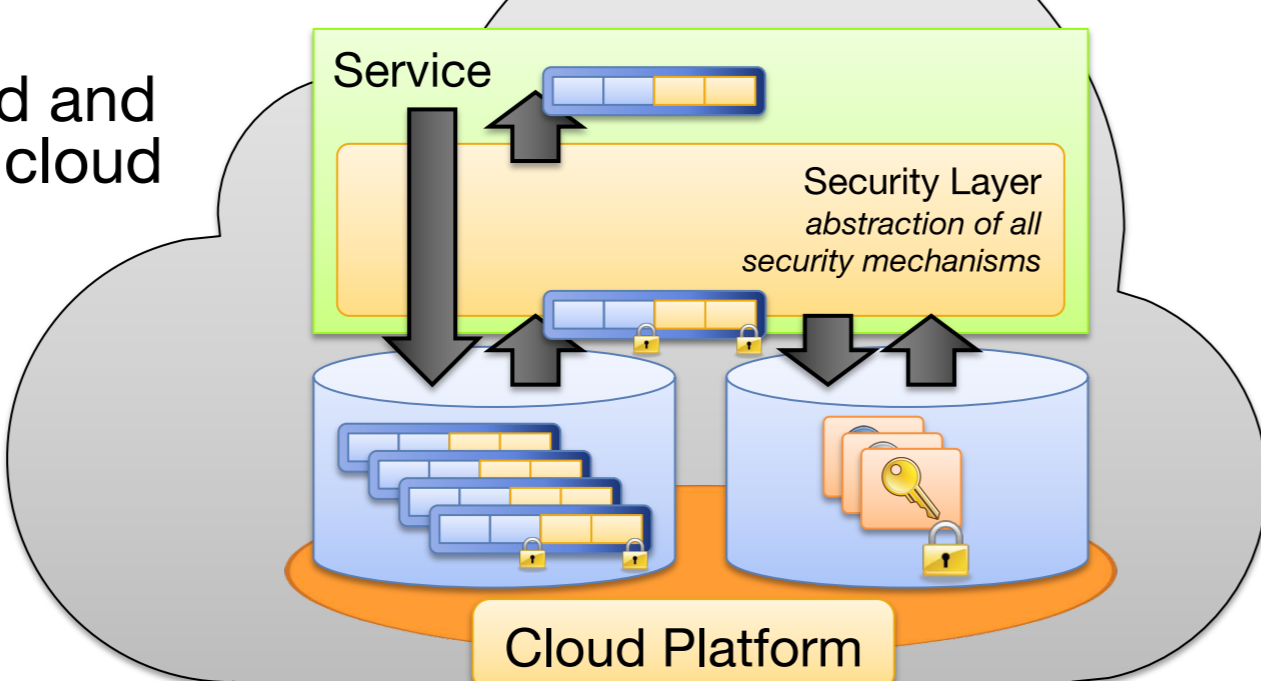
Cloud Platform

Decentralizing Services

Bob's Decentralized Cloud

Internet

Bob

Alice

Alice's Decentralized Cloud

- Realize basic cloud functionality over distributed trusted resources
  - ‣ Peer-to-peer cloud platform utilizes idle resources of devices operated by users' friends and family
  - ‣ Strong isolation of services and data ensures security in multi-tenancy situations
  - ‣ Compatibility with Google App Engine eases migration away from public cloud services
  - ‣ Alternative to today's public cloud offers for extremely privacy-conscious users

Further Reading

Dr. Martin Henze
https://www.comsys.rwth-aachen.de

COM SYS | RWTH AACHEN UNIVERSITY