TEK5530 - Measurable Security for the Internet of Things

L14 – Cloud basics

György Kálmán,
DNB/UiO ITS
gyorgy.kalman@its.uio.no

Josef Noll
UiO ITS
josef.noll@its.uio.no

1

http://cwi.unik.no/wiki/TEK5530, *#IoTSec*, *#IoTSecNO*

TEK5530: Lecture plan

- 17.01 L1: Introduction
- 24.01
  - L2: Internet of Things
- 31.01
  - L3: Security of IoT + Paper list
- 07.02
  - L4: Smart Grid, Automatic Meter Readings
  - L5: Service implications on functional requirements
- 14.02
  - L6: Technology mapping
  - L9: Top 20 critical security controls
- 21.02 --- Winter holiday
  - «homework» see recording of
  L7: Practical implementation of ontologies
- 28.02
  - L8: Paper analysis with 25 min presentation
  - L10: Intrusion detection

- 07.03
  - L13: Communication and security in current industrial automation
  - L14: Cloud basics and cloud architecture
- 14.03
  - L11: Multi-Metrics Method for measurable Security
  - L12: Multi-Metrics Weighting of an AMR sub-system
- 21.03
  - L15: Cloud security, IoT and service examples from AWS
  - L16: Cloud monitoring, automation and incident response
- 28.03
  - L17: Selected recent topics from IoT security
  - L18: Wrap-up of the course
- 04.04 ---- No lecture, prepare for exam, consultation possibility
- 11.04 ---- No lecture, prepare for exam, consultation possibility or Exam (depending on what we agree on)
- 18.04 ---- Easter holiday, no lecture
- 25.04 ---- Exam

Cloud – Security – IoT

- What is cloud computing
- Delivery models and shared responsibility
- Cloud architecture
- Recommended additional resources

What is cloud computing

- A remote pool of (shared) resources on different levels
- Dynamic provisioning, elastic use of resources, pay-as-you-go
- A type of outsourcing

- Increased utilization of resources, economy of scale
- Multi-tenancy
- Global reach
- Running expense vs capital expense
- High availability – but assumes (fast) internet connectivity
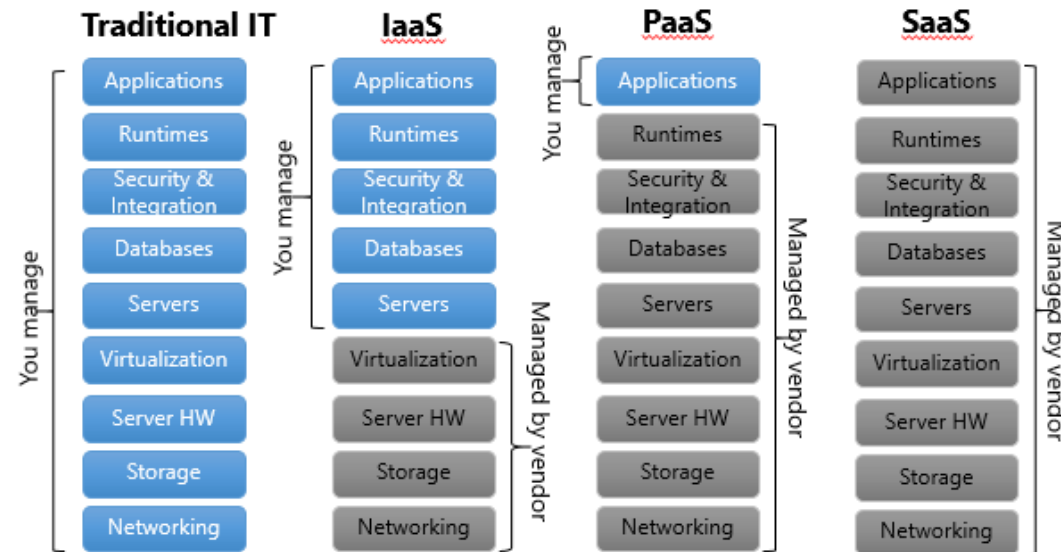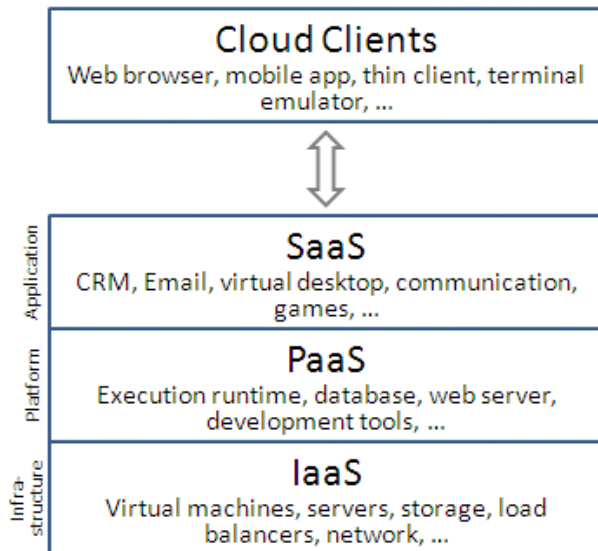- Deployment: public, private, hybrid and community

Figure from https://www.slideshare.net/AmazonWebServices/awsome-day-nashville-2018training

Delivery models

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)

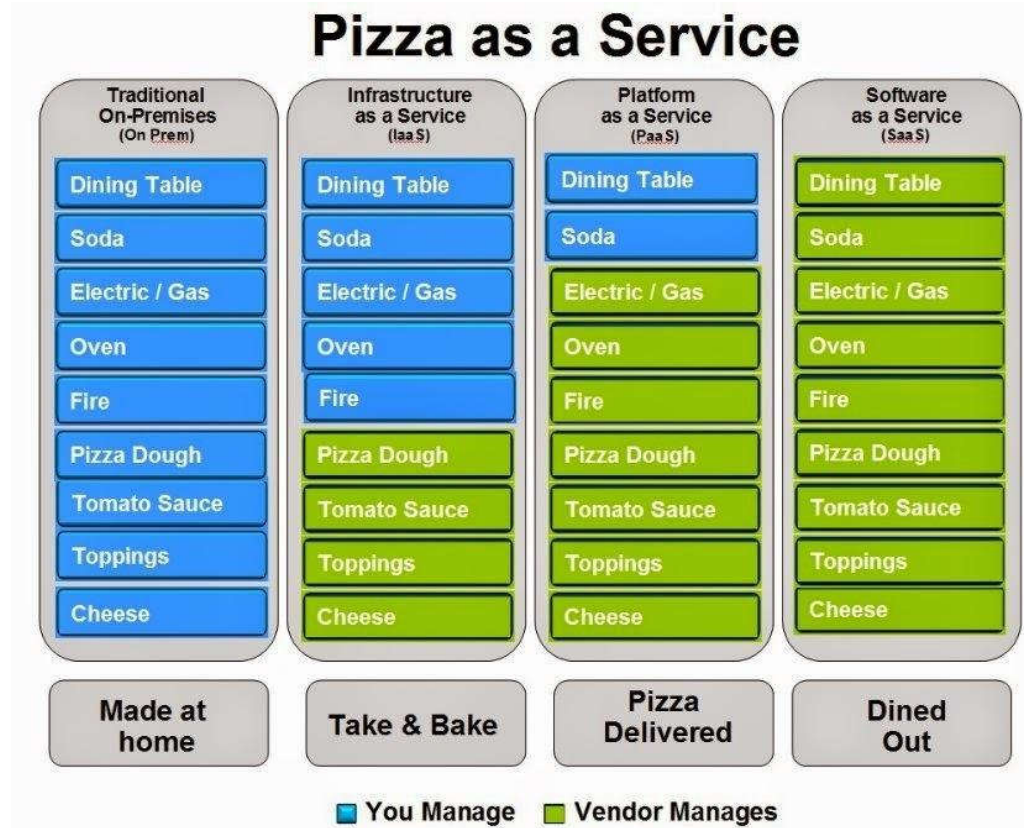*Both figures are from: http://oracle-help.com/oracle-cloud/cloud-computing-stack-saas-paas-iaas/*

Delivery models contd.

✎ A perfect figure from Fred Bals at Episerver

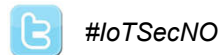https://www.episerver.com/learn/resources/blog/fred-bals/pizza-as-a-service/

Delivery models contd.

- On demand, self-service provisioning
- Virtual workspaces
- Xen with para-virtualization (near-native performance, live migration)
- Patch management, golden images, instant update

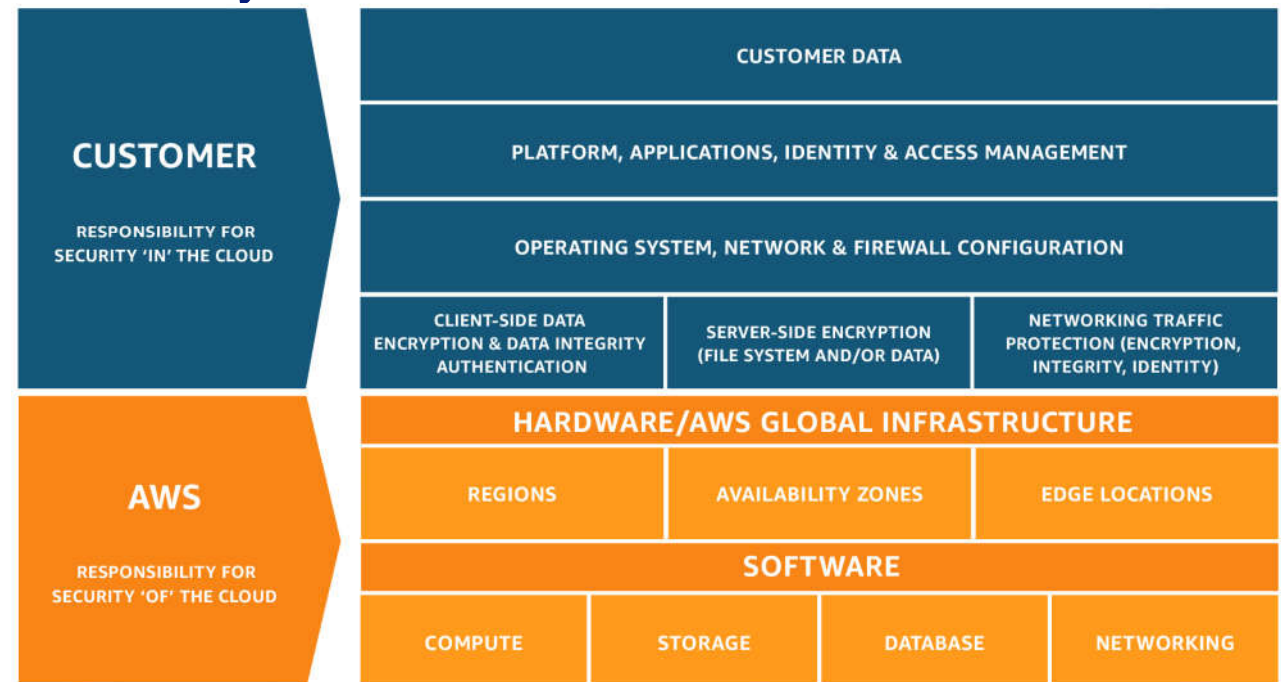*https://www.episerver.com/learn/resources/blog/fred-bals/pizza-as-a-service/*

AWS Shared Responsibility Model

- AWS responsibility is to provide a reliable and secure infrastructure, where the customer services can be built on, a «foundation»
- Customer responsibility is determined by the services chosen
- Wide range of services
- And third party deliveries

CUSTOMER RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD	CUSTOMER DATA		
	PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT		
	OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION		
	CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION	SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)	NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)
AWS RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD	HARDWARE/AWS GLOBAL INFRASTRUCTURE		
	REGIONS	AVAILABILITY ZONES	EDGE LOCATIONS
	SOFTWARE		
	COMPUTE	STORAGE	DATABASE	NETWORKING

https://aws.amazon.com/compliance/shared-responsibility-model/

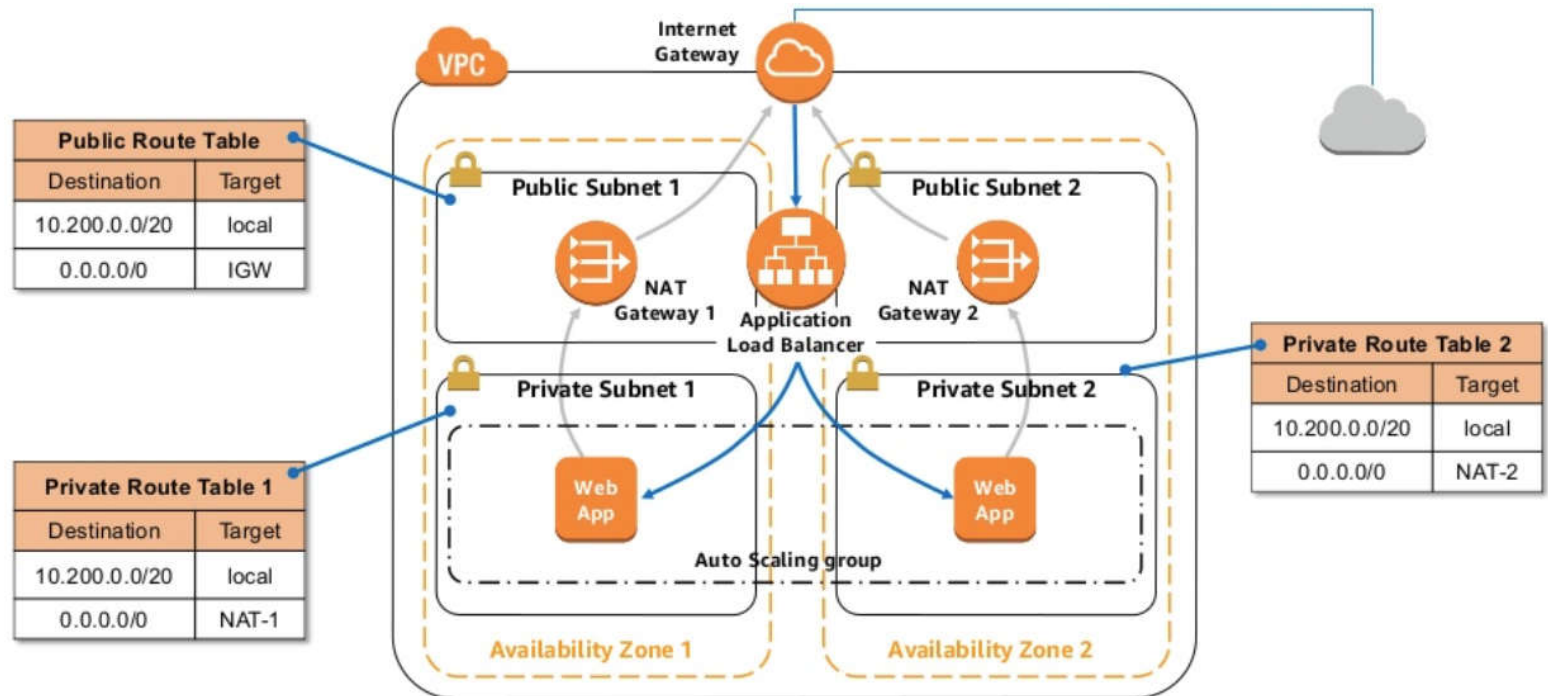UNIK4750   #IoTSecNO   *March 2018, György Kálmán, Josef Noll*

Fundamentals

- Edge location
  - Border towards CloudFront, AWS' Content Delivery Network
  - Supports AWS DNS service (Route 53), WAF, Shield, Lambda@Edge
- Basic components
  - EC2
  - S3
  - VPC
- AWS Marketplace: a Play store for your cloud installation

Generic service architecture