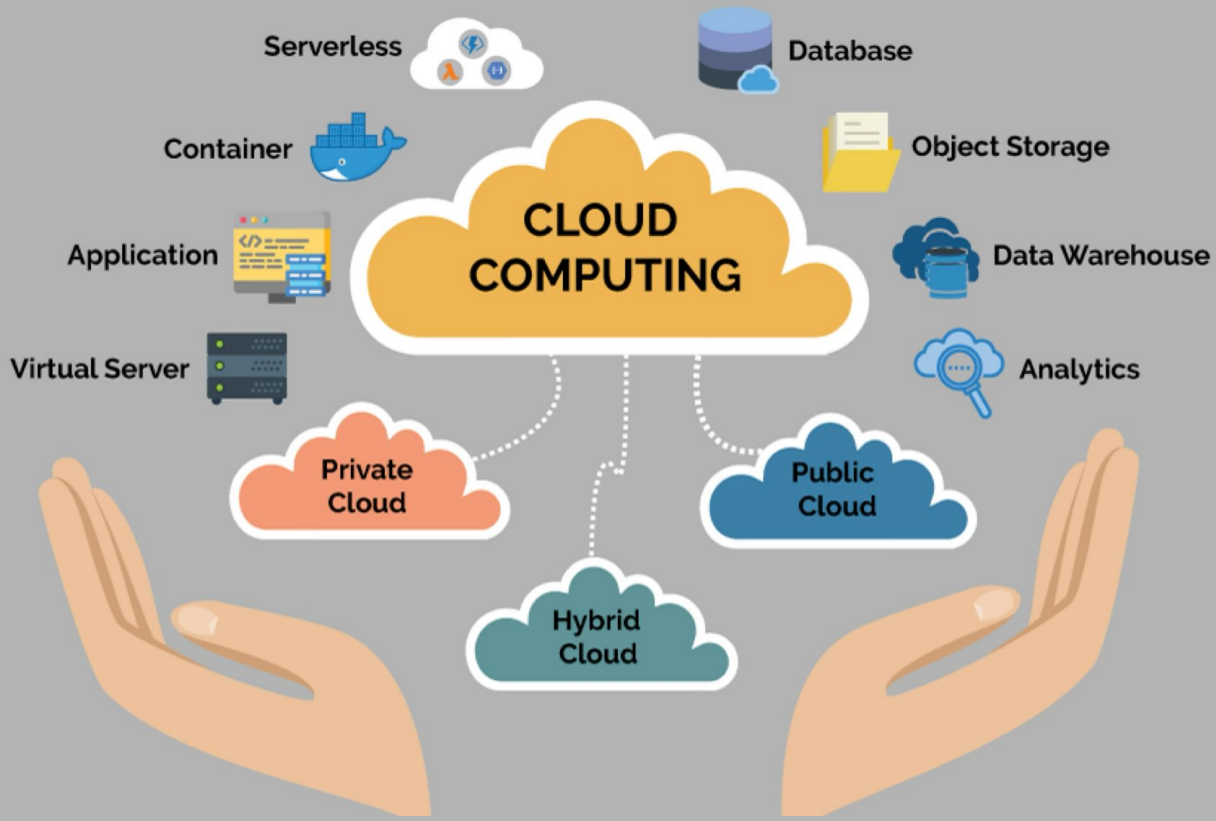
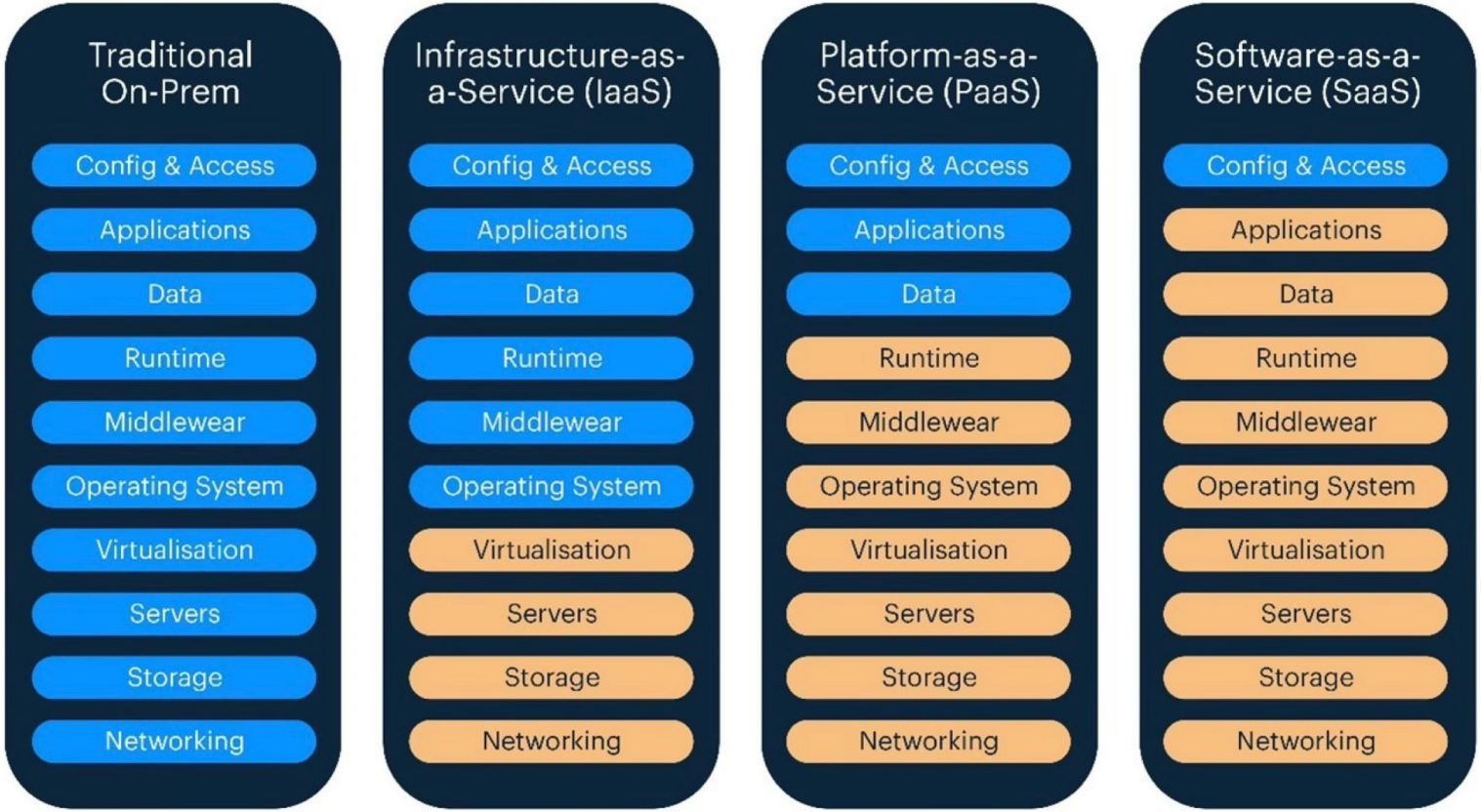
Prof. Alessandro Carrega
alessandro.carrega@unige.it

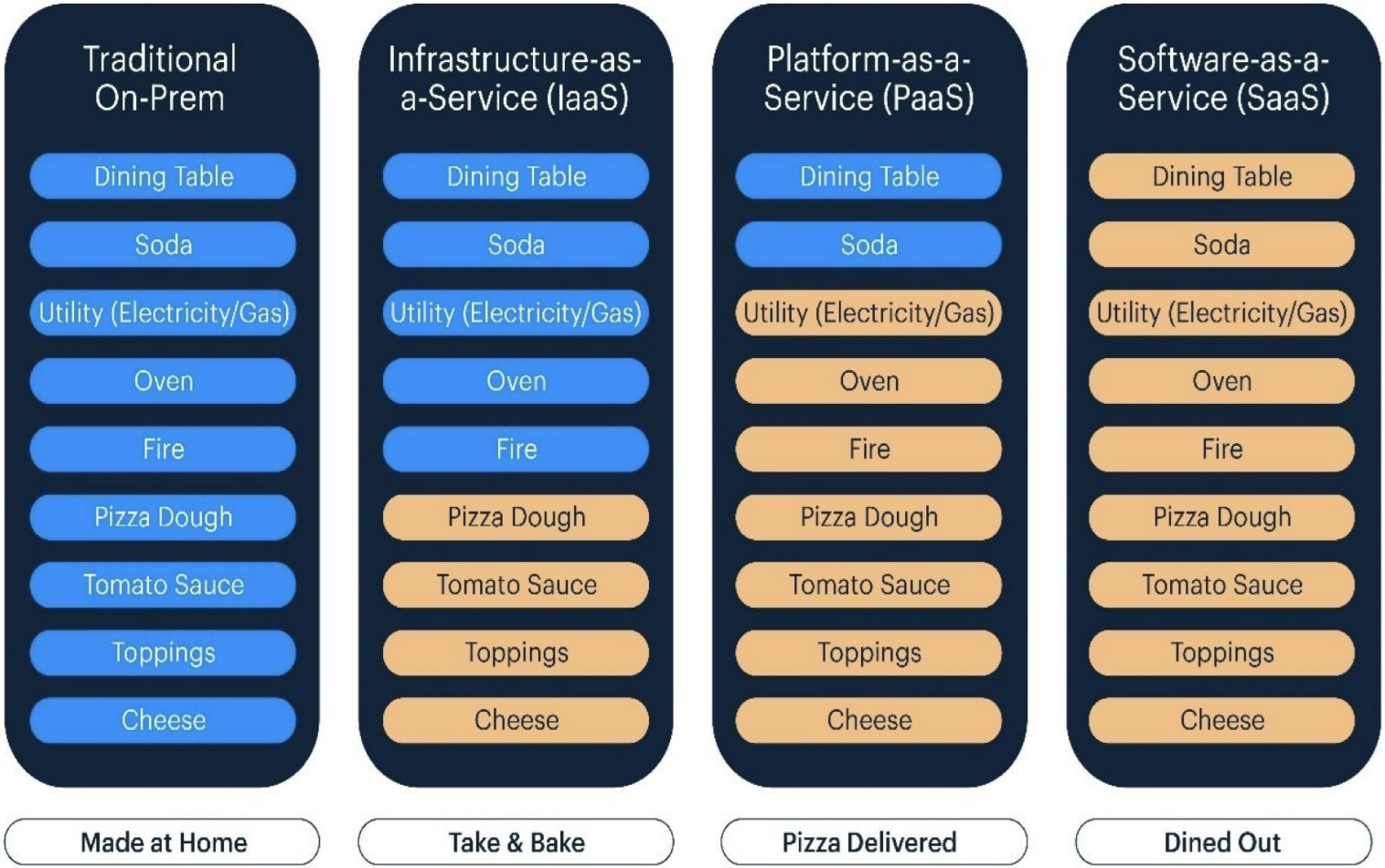
Lesson 01

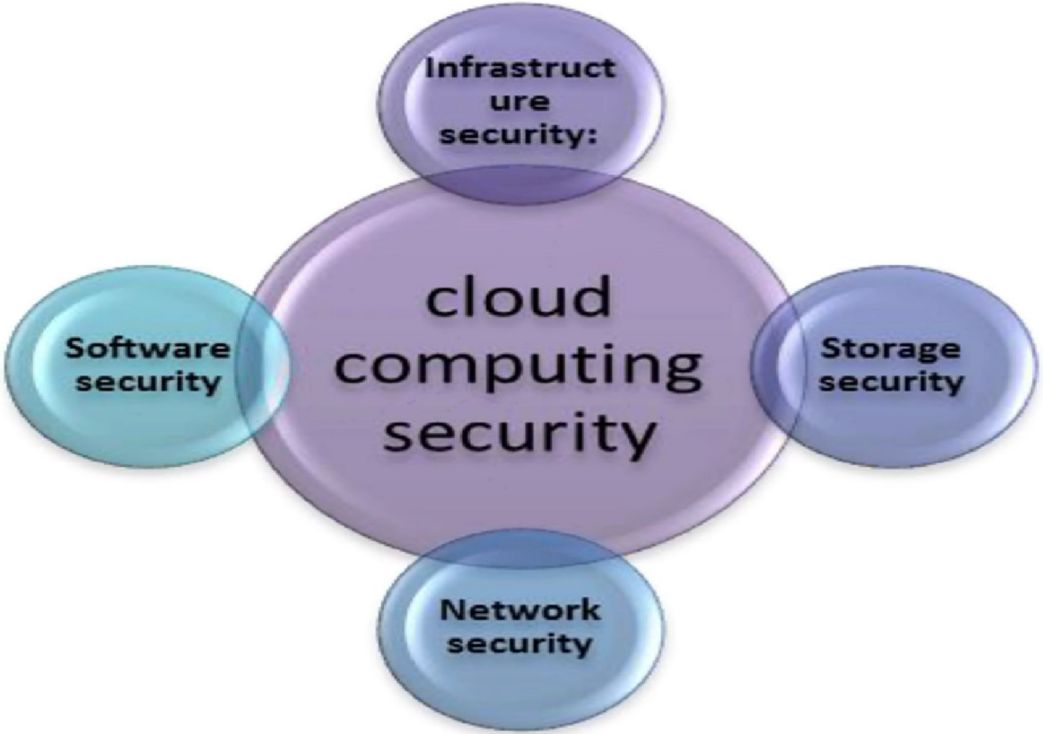
Welcome & Context

Ph.D. Course in Cyber Security for Cloud Computing
from zero to hero


Serverless
Database
Container
Object Storage
CLOUD COMPUTING
Application
Data Warehouse
Virtual Server
Analytics
Private Cloud
Public Cloud
Hybrid Cloud

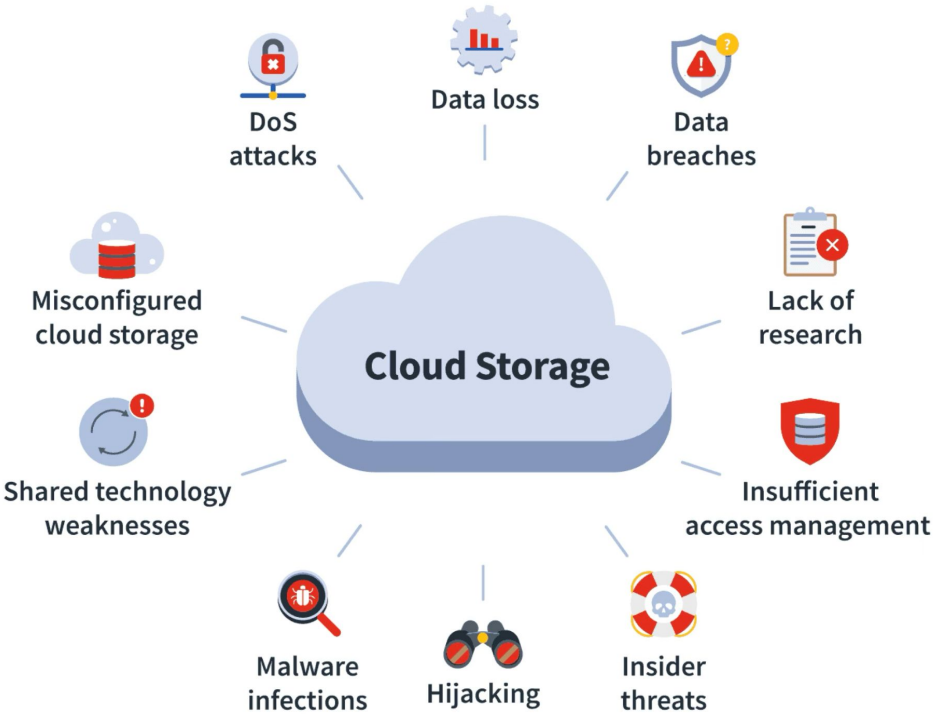

Traditional On-Prem
Config & Access
Applications
Data
Runtime
Middlewear
Operating System
Virtualisation
Servers
Storage
Networking
Infrastructure-as-a-Service (IaaS)
Config & Access
Applications
Data
Runtime
Middlewear
Operating System
Virtualisation
Servers
Storage
Networking
Platform-as-a-Service (PaaS)
Config & Access
Applications
Data
Runtime
Middlewear
Operating System
Virtualisation
Servers
Storage
Networking
Software-as-a-Service (SaaS)
Config & Access
Applications
Data
Runtime
Middlewear
Operating System
Virtualisation
Servers
Storage
Networking

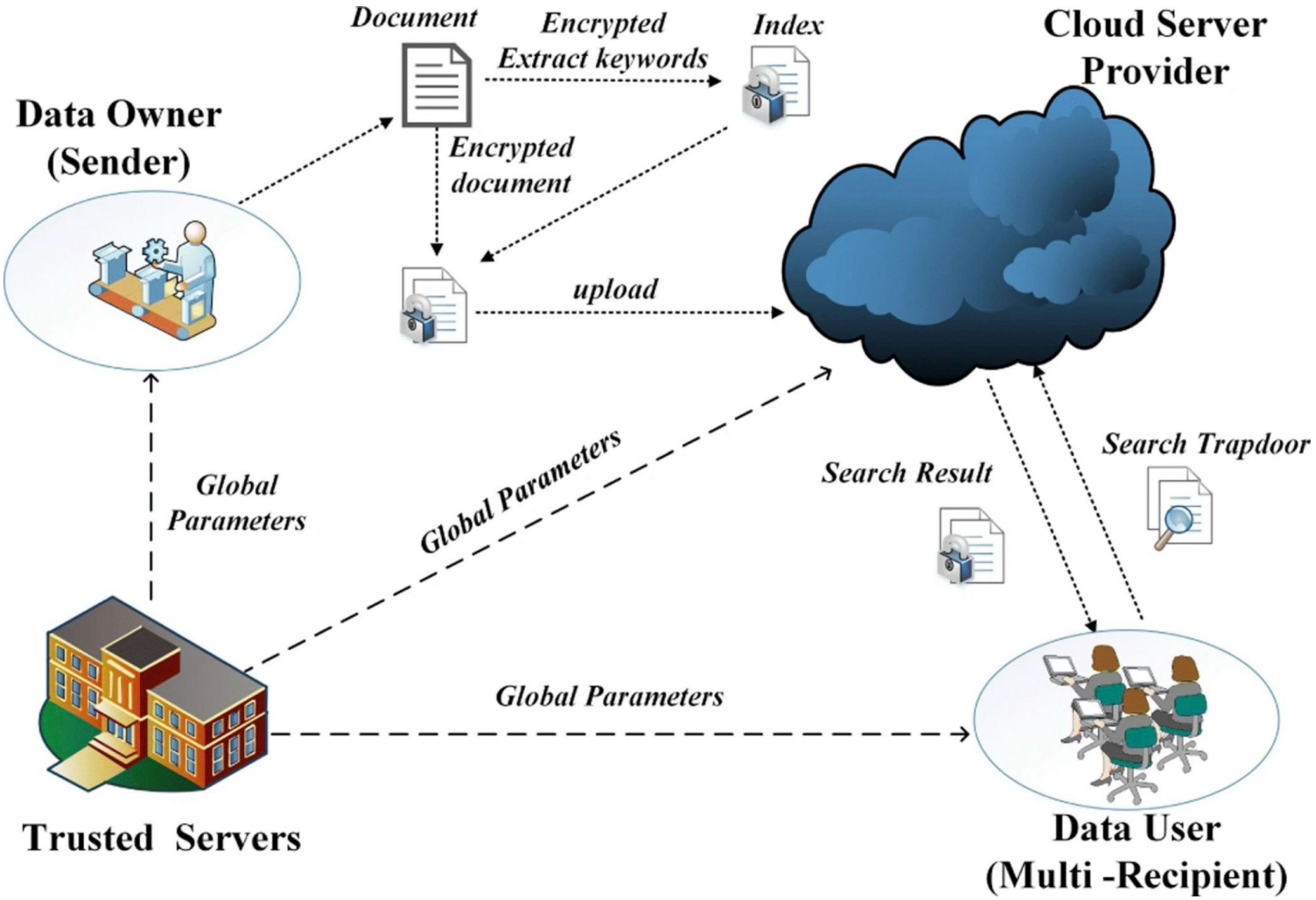

Traditional On-Prem
Dining Table
Soda
Utility (Electricity/Gas)
Oven
Fire
Pizza Dough
Tomato Sauce
Toppings
Cheese
Made at Home
Infrastructure-as-a-Service (IaaS)
Dining Table
Soda
Utility (Electricity/Gas)
Oven
Fire
Pizza Dough
Tomato Sauce
Toppings
Cheese
Take & Bake
Platform-as-a-Service (PaaS)
Dining Table
Soda
Utility (Electricity/Gas)
Oven
Fire
Pizza Dough
Tomato Sauce
Toppings
Cheese
Pizza Delivered
Software-as-a-Service (SaaS)
Dining Table
Soda
Utility (Electricity/Gas)
Oven
Fire
Pizza Dough
Tomato Sauce
Toppings
Cheese
Dined Out

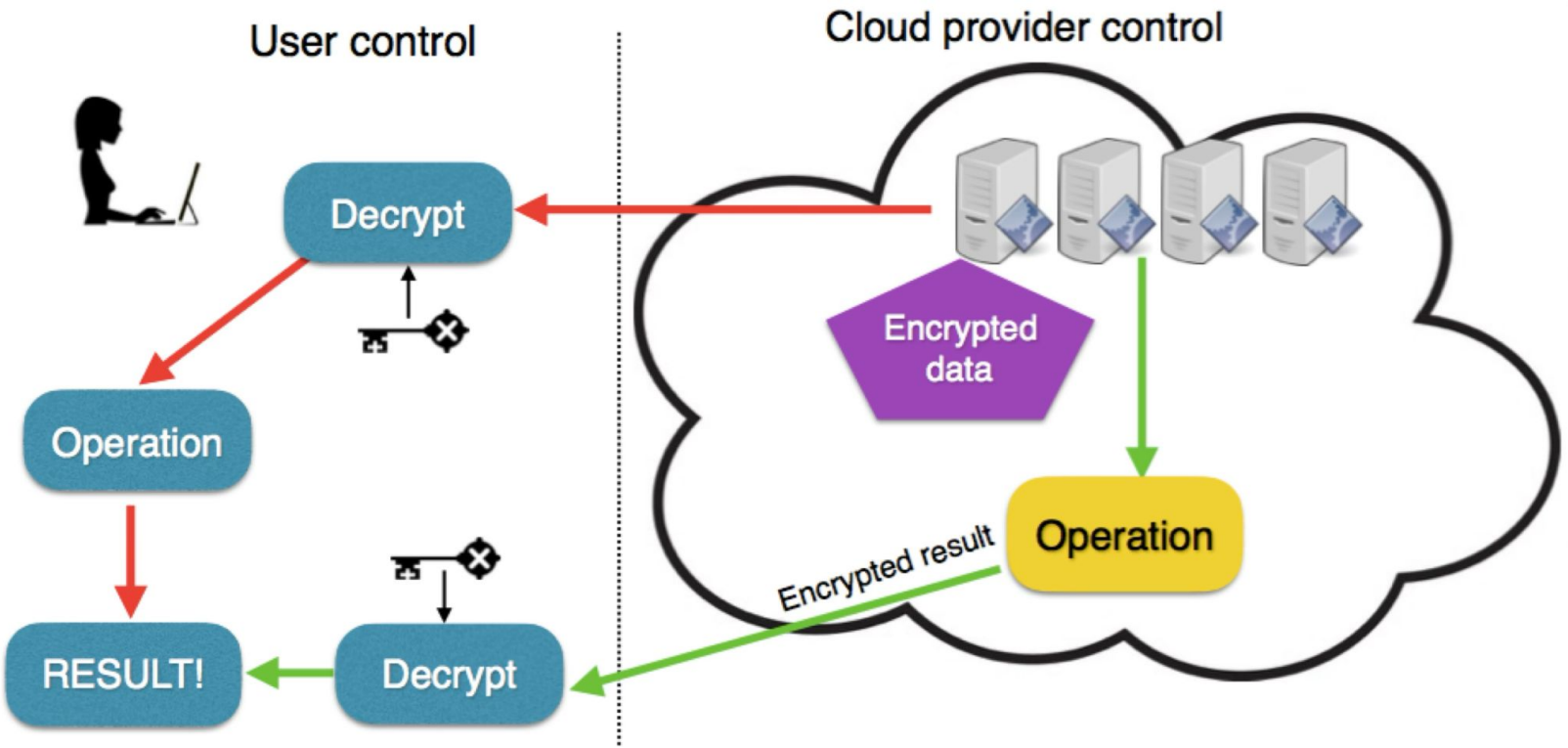

Infrastructure security:
cloud computing security
Software security
Storage security
Network security

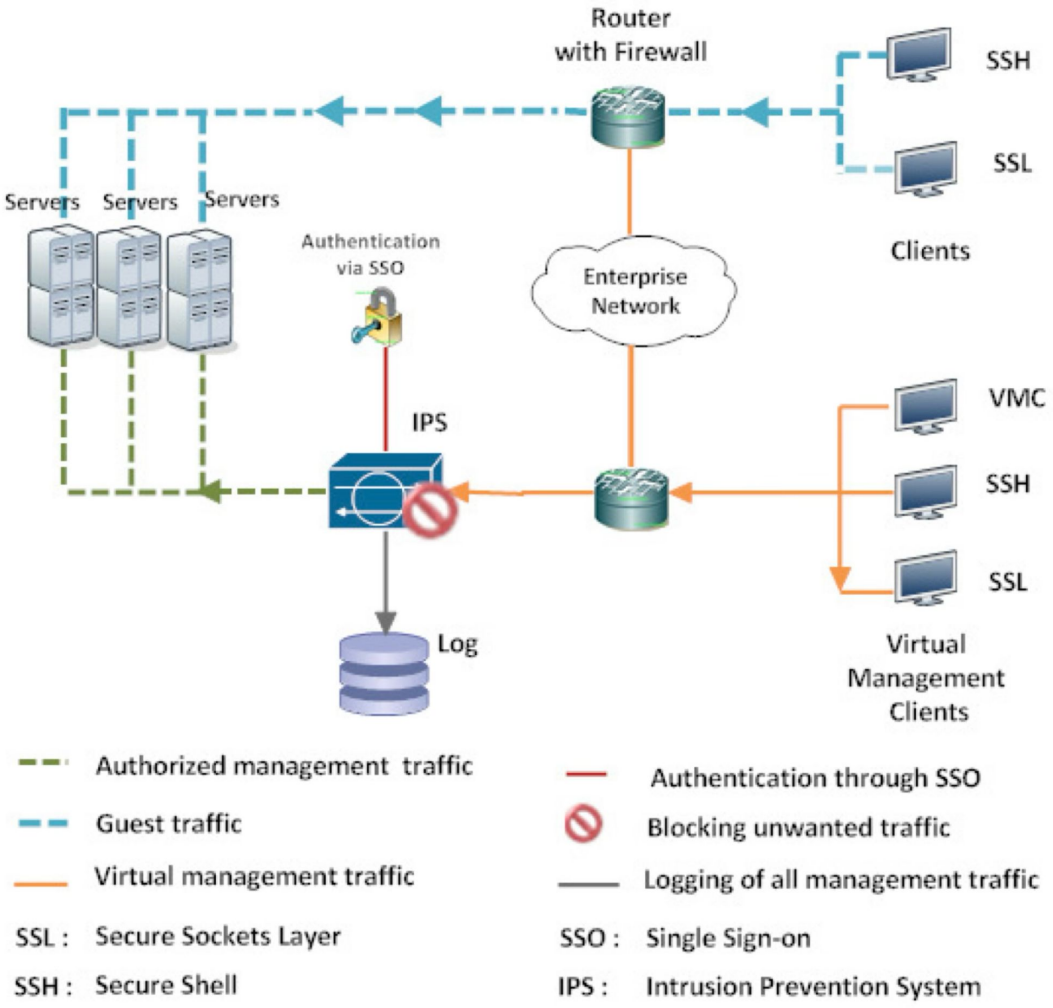

Governance
Compliance
Availability
Data Security
Identity and Access Management
DR/BC Planning
Cloud Security

Cloud Security Risks You Need To Know



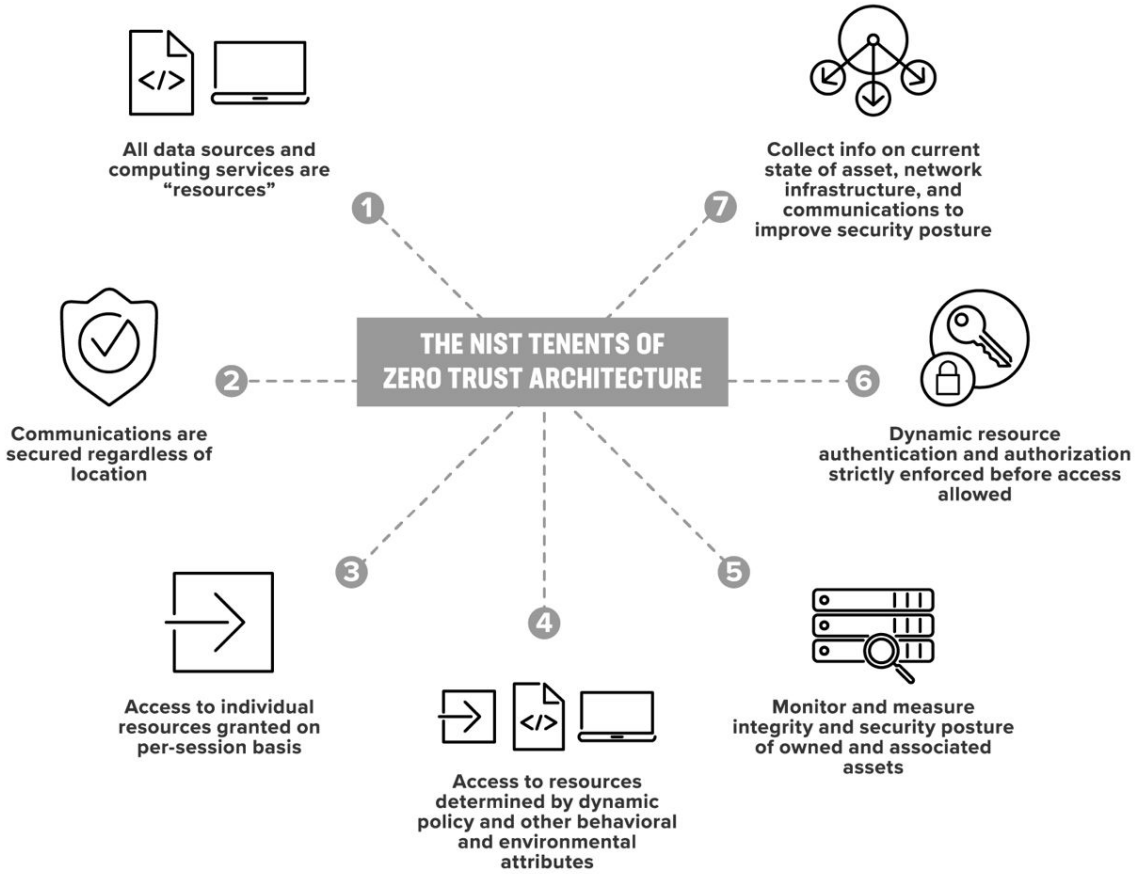

Document
Encrypted
Extract keywords
Index
Cloud Server
Provider
Data Owner
(Sender)
Encrypted
document
upload
Global
Parameters
Global Parameters
Search Result
Search Trapdoor
Global Parameters
Trusted Servers
Data User
(Multi -Recipient)

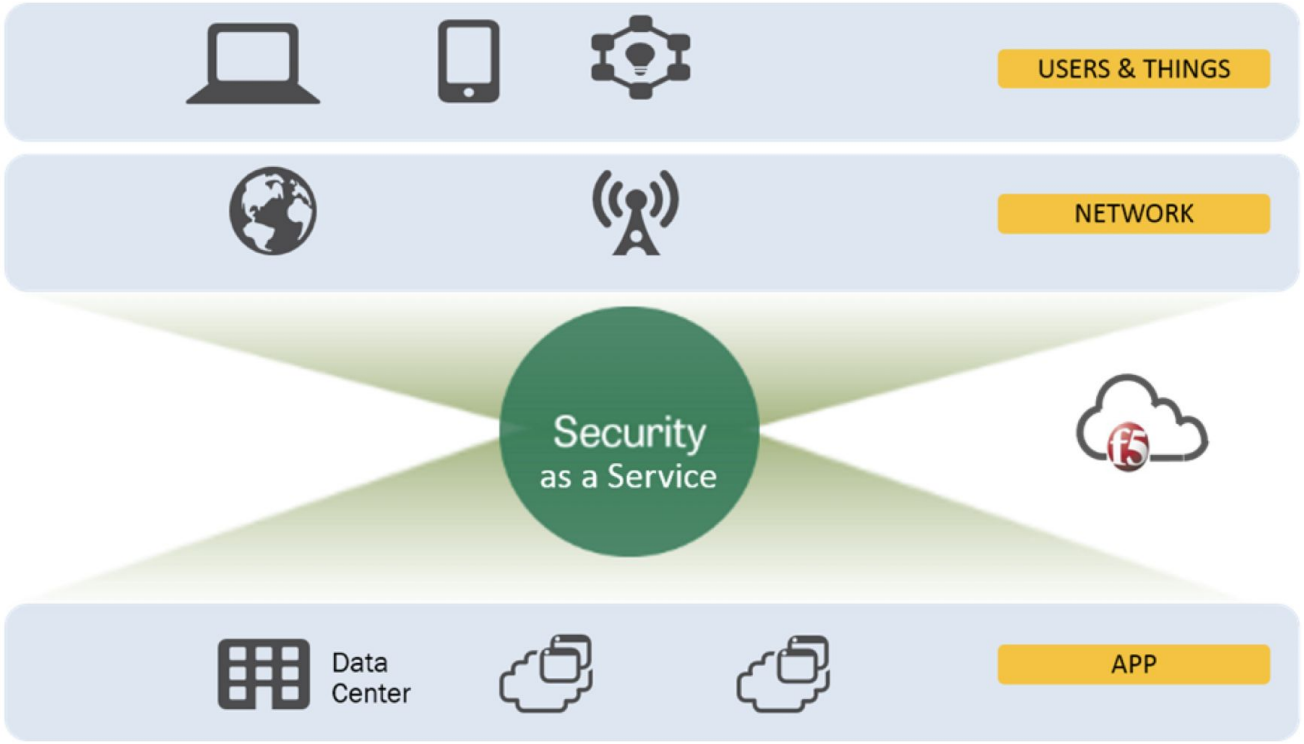

User control
Cloud provider control
Decrypt
Encrypted data
Operation
Operation
Encrypted result
RESULT!
Decrypt


Router
with Firewall
SSH
SSL
Clients
Servers
Servers
Servers
Authentication
via SSO
Enterprise
Network
IPS
VMC
SSH
SSL
Log
Virtual
Management
Clients
Authorized management traffic
Guest traffic
Virtual management traffic
SSL : Secure Sockets Layer
SSH : Secure Shell
Authentication through SSO
Blocking unwanted traffic
Logging of all management traffic
SSO : Single Sign-on
IPS : Intrusion Prevention System

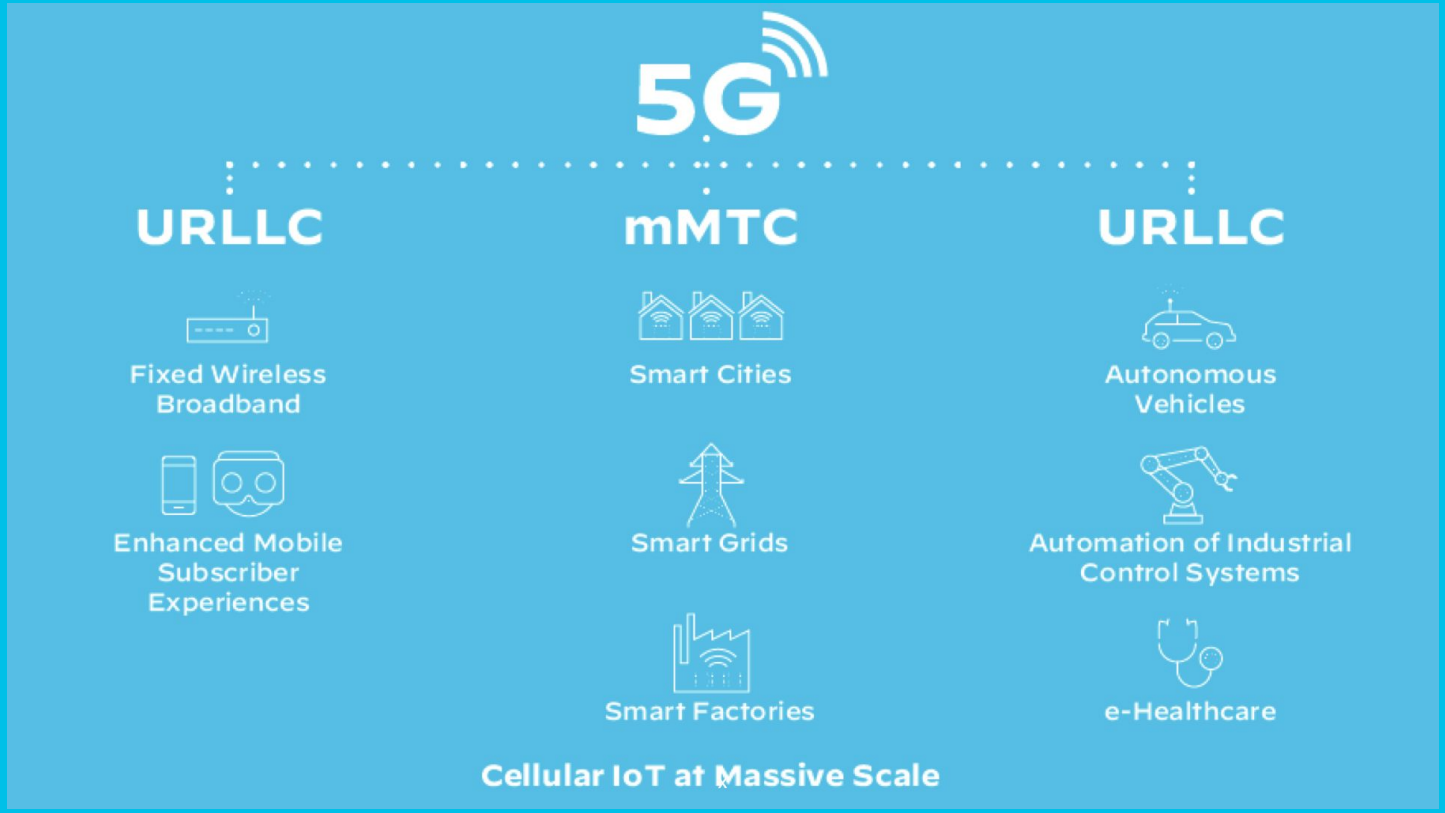
Your Responsibility
for Security (IN)
ther Cloud

CPS Responsibility
for the Security (OF)
the Cloud


THE NIST TENENTS OF ZERO TRUST ARCHITECTURE
1
All data sources and computing services are “resources”
2
Communications are secured regardless of location
3
Access to individual resources granted on per-session basis
4
Access to resources determined by dynamic policy and other behavioral and environmental attributes
5
Monitor and measure integrity and security posture of owned and associated assets
6
Dynamic resource authentication and authorization strictly enforced before access allowed
7
Collect info on current state of asset, network infrastructure, and communications to improve security posture

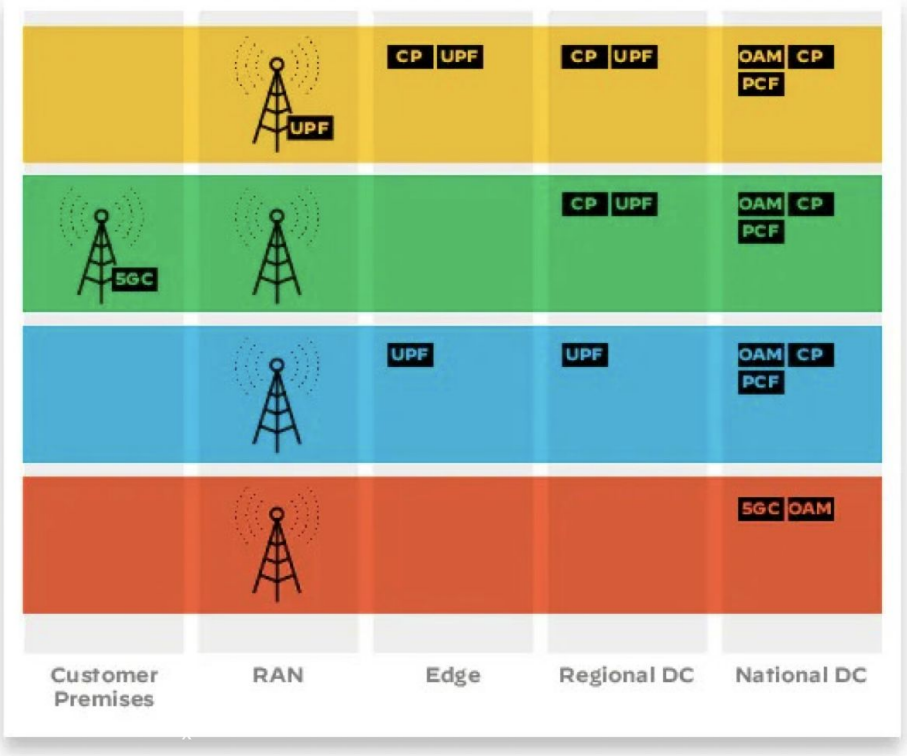

USERS & THINGS
NETWORK
Security
as a Service
Data
Center
APP

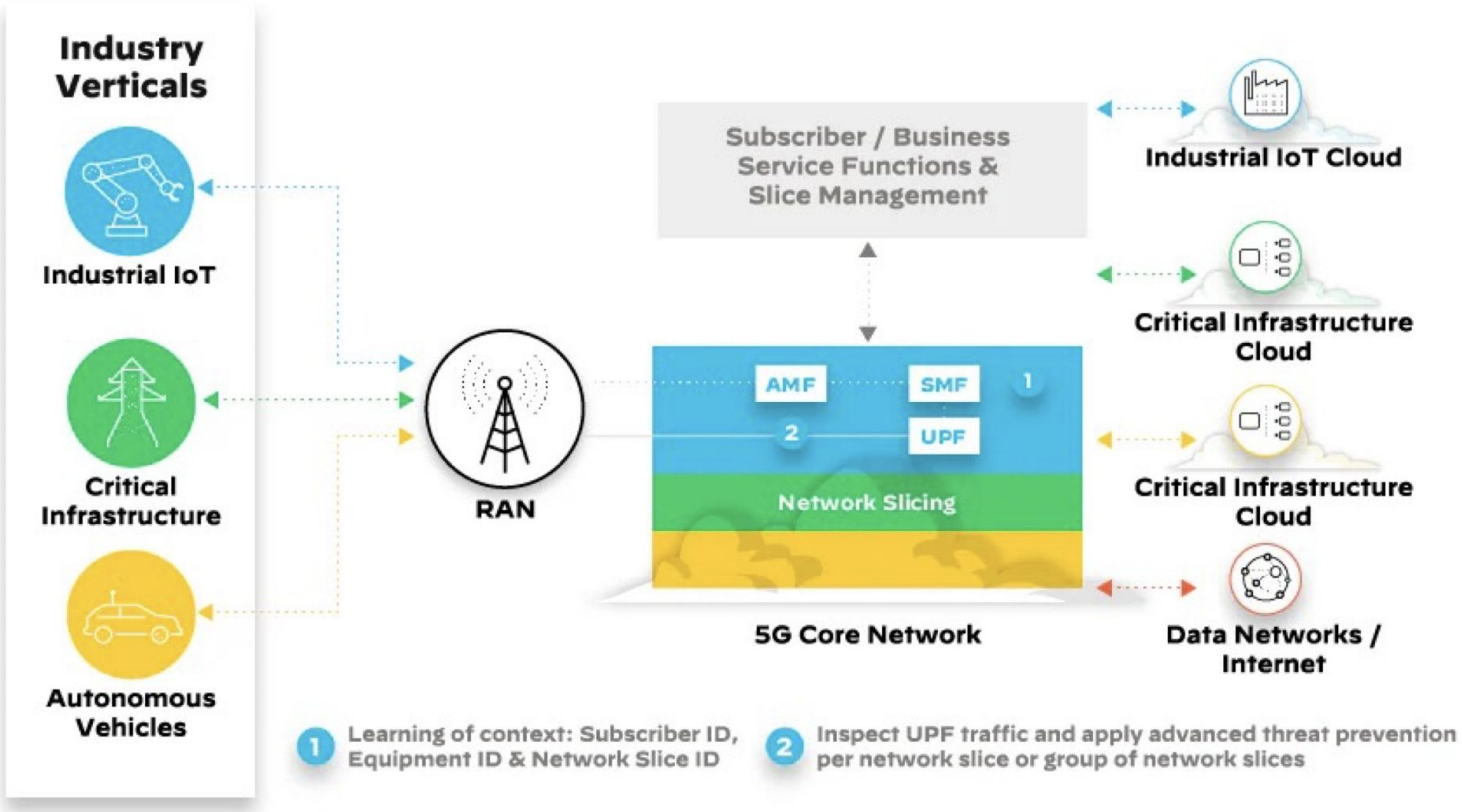

6
To reach ideal security levels, there are six additional security controls that can be built into 5G according to industry standards
4
It's recommended to complement the 10 mandatory controls with 4 more security controls, which can be provided by the MNO or cloud provider
10
There are ten mandatory security controls required to ensure a zero-trust architecture for 5G critical infrastructure in the cloud.


5G
URLLC
mMTC
URLLC
Fixed Wireless Broadband
Enhanced Mobile Subscriber Experiences
Smart Cities
Smart Grids
Smart Factories
Autonomous Vehicles
Automation of Industrial Control Systems
e-Healthcare
Cellular IoT at Massive Scale

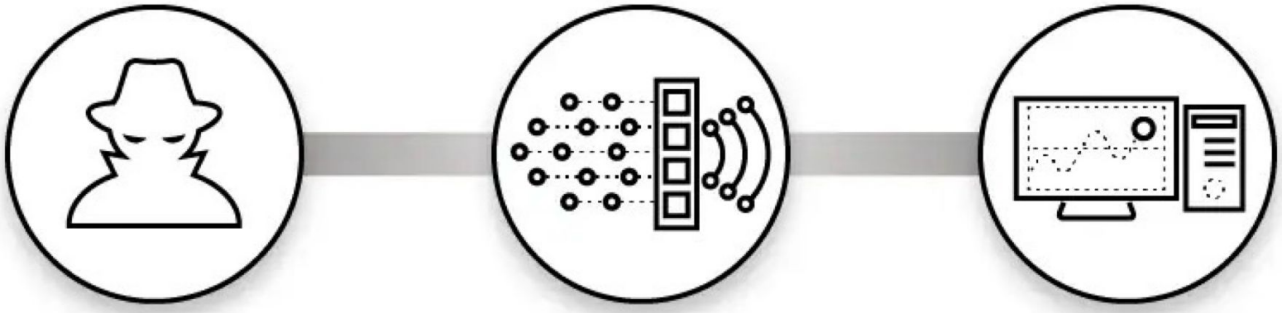
4G LTE	5G
Consumer	Enterprise & Public Sector
Smartphone	IoT, OT, AR/VR, FWA
One-Size-Fits-All	Customized Services
Connect to Internet	Connect to Enterprise Network
Centralized	Distributed to Edge
Bare Metal or Virtual	Cloud-Native

Use Case	Requirements
Critical IoT URLLC	Very High Available Very Low Latency
Enterprise IoT	High Available Low Latency
Enhanced MBB	Wide Area Coverage High Throughput
Massive IoT	Low Cost Low Energy High # of devices




Industry Verticals
Industrial IoT
Critical Infrastructure
Autonomous Vehicles
RAN
Subscriber / Business Service Functions & Slice Management
AMF
SMF
1
2
UPF
Network Slicing
5G Core Network
Industrial IoT Cloud
Critical Infrastructure Cloud
Critical Infrastructure Cloud
Data Networks / Internet
1 Learning of context: Subscriber ID, Equipment ID & Network Slice ID
2 Inspect UPF traffic and apply advanced threat prevention per network slice or group of network slices

How A Side-channel Attack Works



Attacker uses collected data to reconstruct target process

Attacker intercepts emissions

Target computer emits electromagnetic wave

End of Lesson

Q/A