IoT Academy

Digital Transformation: Enhancing IoT-driven Solutions for Smart Islands

Security considerations for smart islands

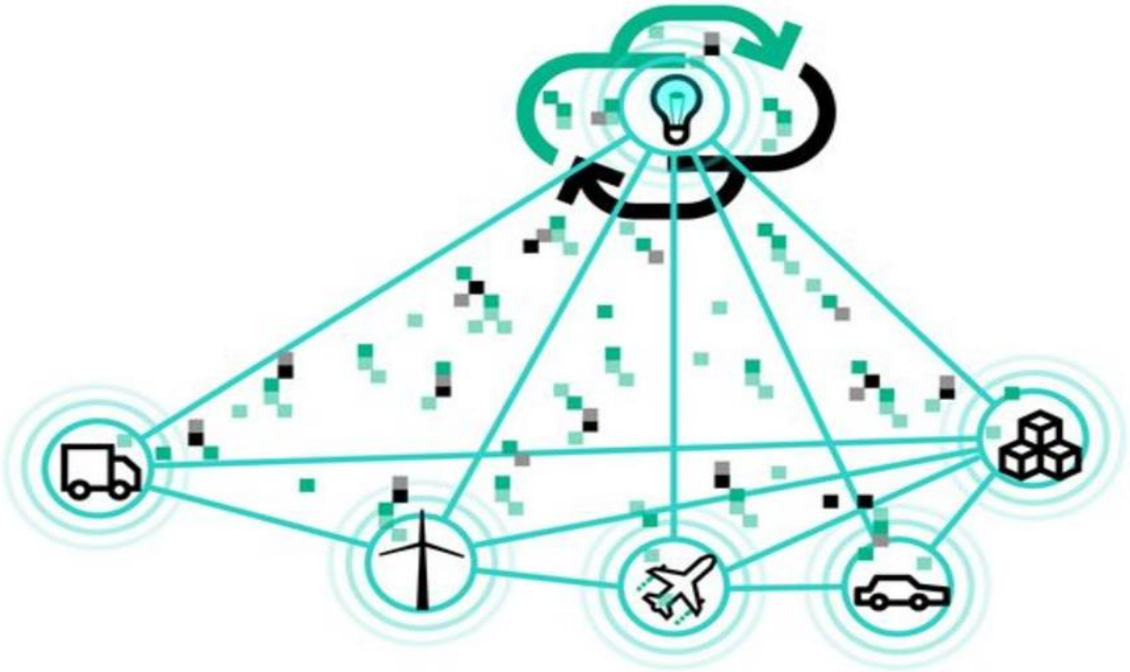
Mostafa Nikpour Kermanian
Certified Information Security Officer
RQ Bank
mostafa.nickpour@gmail.com

Mostafa Nikpour

- Master of Computer Science
- Information Security Consultant
- Producer of security sensors
- Security Hardening solution maker

- https://www.linkedin.com/in/mostafa-nikpour-ba2729a7/

What *is* the Internet of Things?



It's about connected devices, systems, and "things" …

Gartner estimates 26 billion connected devices by 2020.

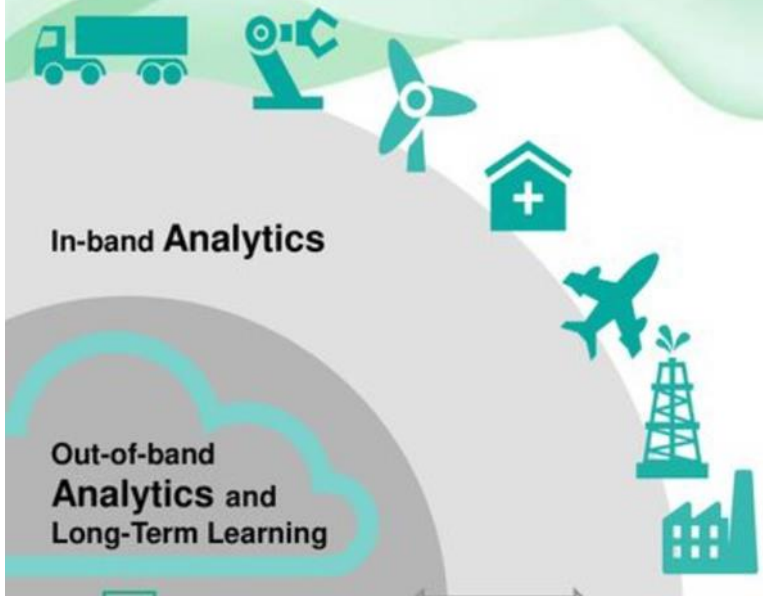
It's about data from the "things …

IDC predicts IoT data will account for 10% of the world's data by 2020.

It's about new insights…

Business, engineering, scientific insights

What *is* the Internet of Things?



Collaboration & Analytics

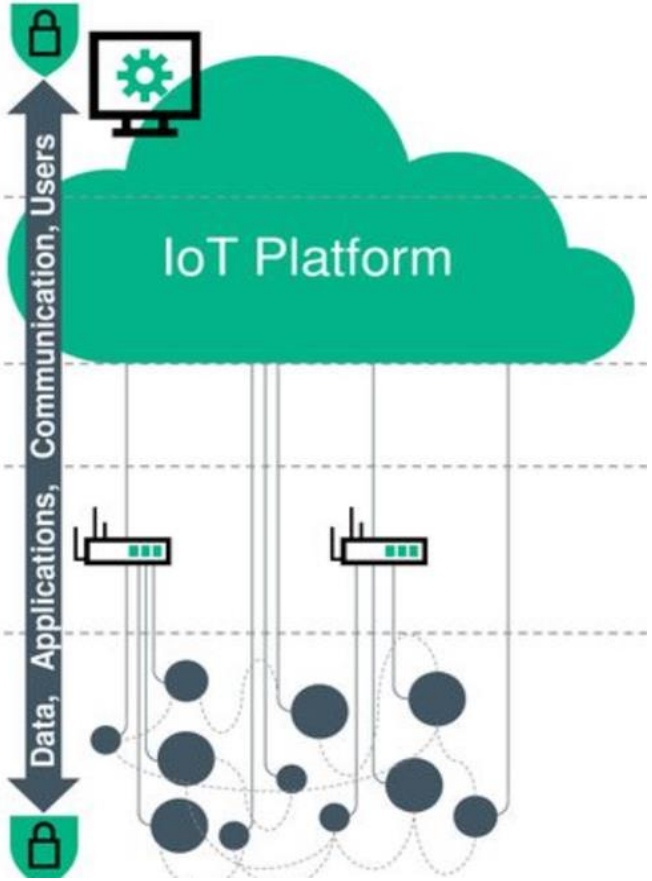
Interconnect Operations Technology (**OT**) and Information Technology (**IT**) to enable Machine to Machine communication (**M2M**) and collaboration.

Collect all **data** and **transform** the business model with **Analytics** to gain **new business insights**.

One single breach though,
can destroy the whole business model!

What are the main IoT Building Blocks that need to be secured?

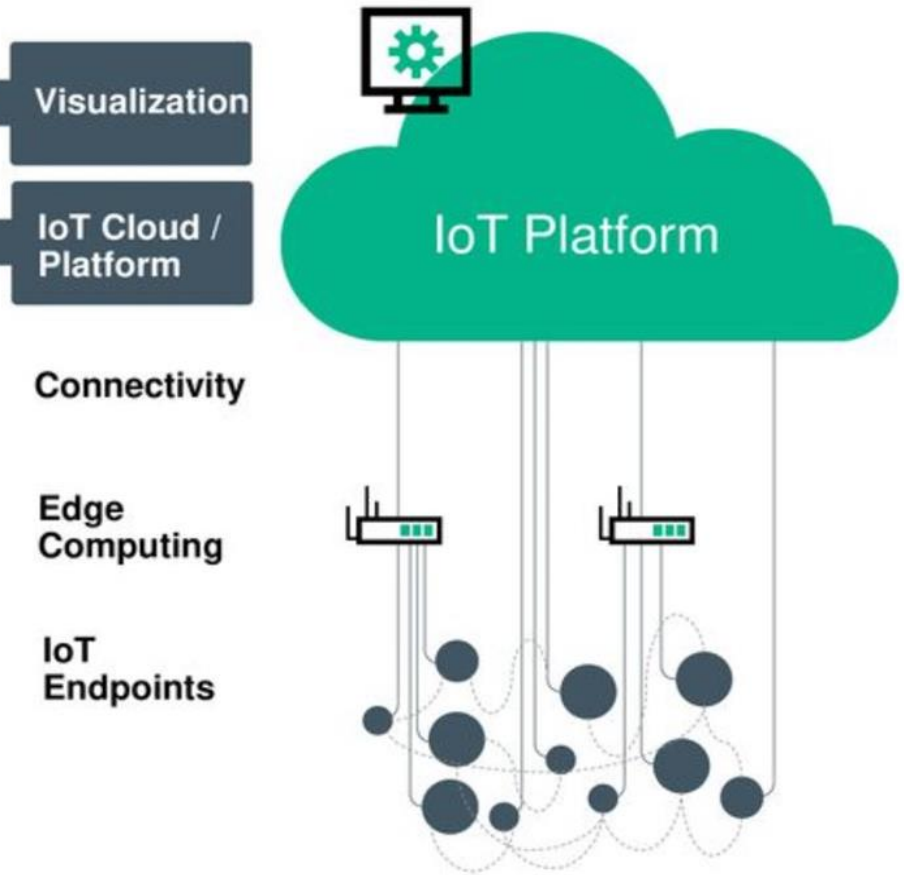
Applications that present and visualize the findings and key performance indicators (KPI). Open ecosystem for partners and suppliers.	**Visualization**
Operations and control of the IoT infrastructure. Central **data storage**. Contextual enrichment, **Big-Data analytics** and (deep) machine learning. Turning Data into insights. Turning insights into Business Transformation.	**IoT Cloud / Platform**
Ubiquitous, reliable and secure **communication** technology for all endpoints and edge devices.	**Connectivity**
Processing unit sitting on the same physical entity (e.g. car, turbine, airplane, building) as the IoT endpoints. Translates the **OT protocol** (e.g. SCADA) to an **IT protocols** (e.g. TCP/IP). Ingests and pre-processes the data (also called **Edge Analytics** or **Real-Time Analytics** or **In-band Analytics**).	**Edge Computing**
Distributed Sensors and **Actuators** - either mobile or stationary but always connected to the IoT cloud via the internet or a private network. IoT endpoints can connect directly or via an edge computing device. IoT endpoints can also communicate to each others (**machine to machine** – M2M)	**IoT Endpoints**



What are the main Attack Scenarios and Risks?

Vulnerable Web Applications and APIs
Vulnerabilities in the IoT clouds web applications and API interfaces can lead to a denial of service, data loss or a complete take over of the application. The most common web application security flaws are listed in the OWASP Top10 and must be protected by all means.

Targeted Attacks
IoT infrastructures are like all other environments for attackers if and when there is sensitive data that can be monetized. Targeted attacks (Advanced Persistent Threats – APT) must be detected as soon as possible to take away what the attackers need most – time to find and exfiltrate/damage the valuable data.

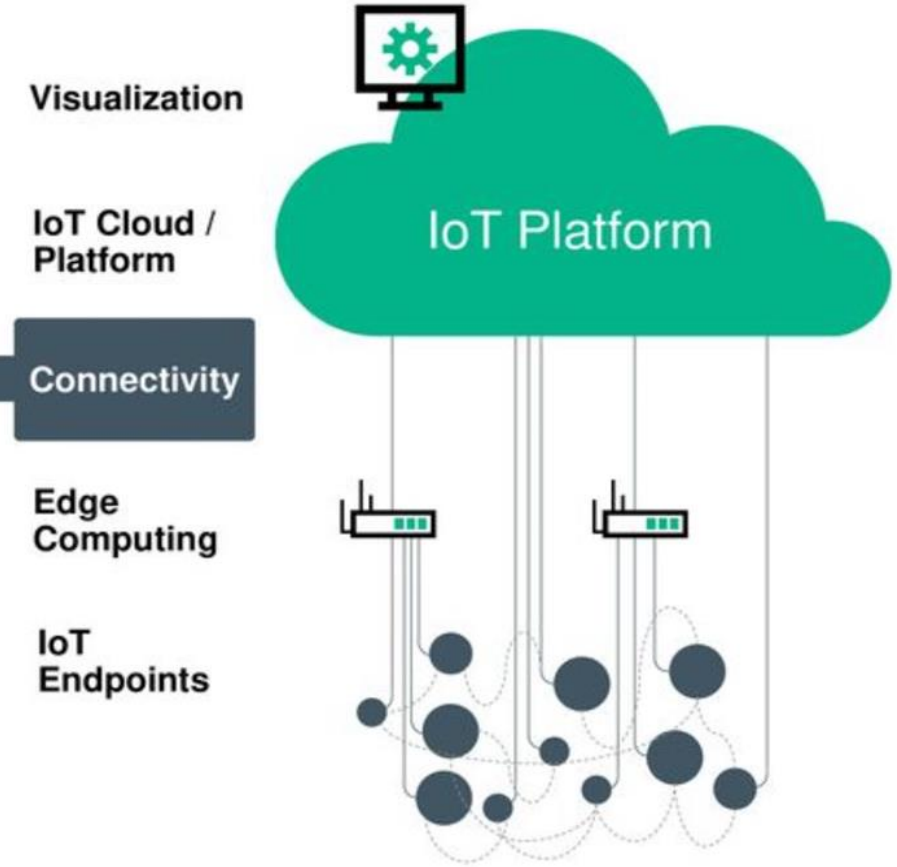


What are the main Attack Scenarios and Risks?

Man-In-The-Middle Attacks (MitM)
Attackers that sneak into the communication between two parties (e.g. IoT Edge and IoT Cloud) who believe they are directly communicating with each other, can cause immense damage to the whole IoT system.

Denial-of-Service Attack (DoS)
IoT cloud services like Web(APIs) portals, VPN can be disrupted and made unavailable temporarily or indefinitely.

Unauthorized Access
By simulating the identity of authorized endpoints, rogue endpoints can sneak their way into the system.

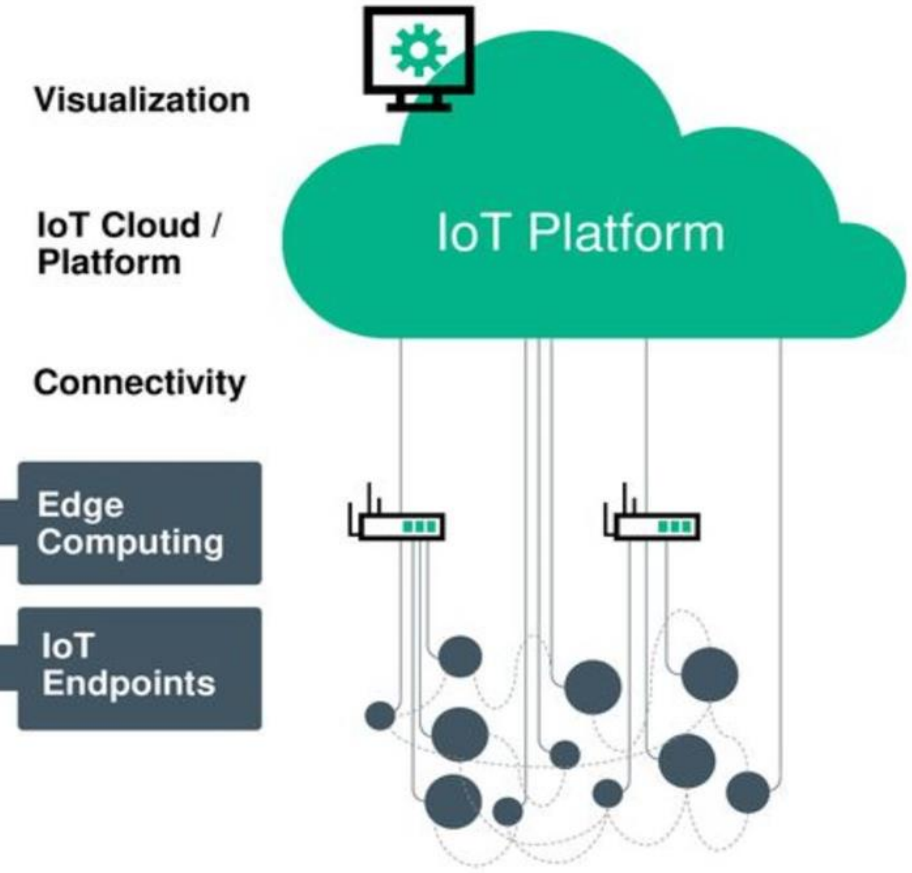


What are the main Attack Scenarios and Risks?

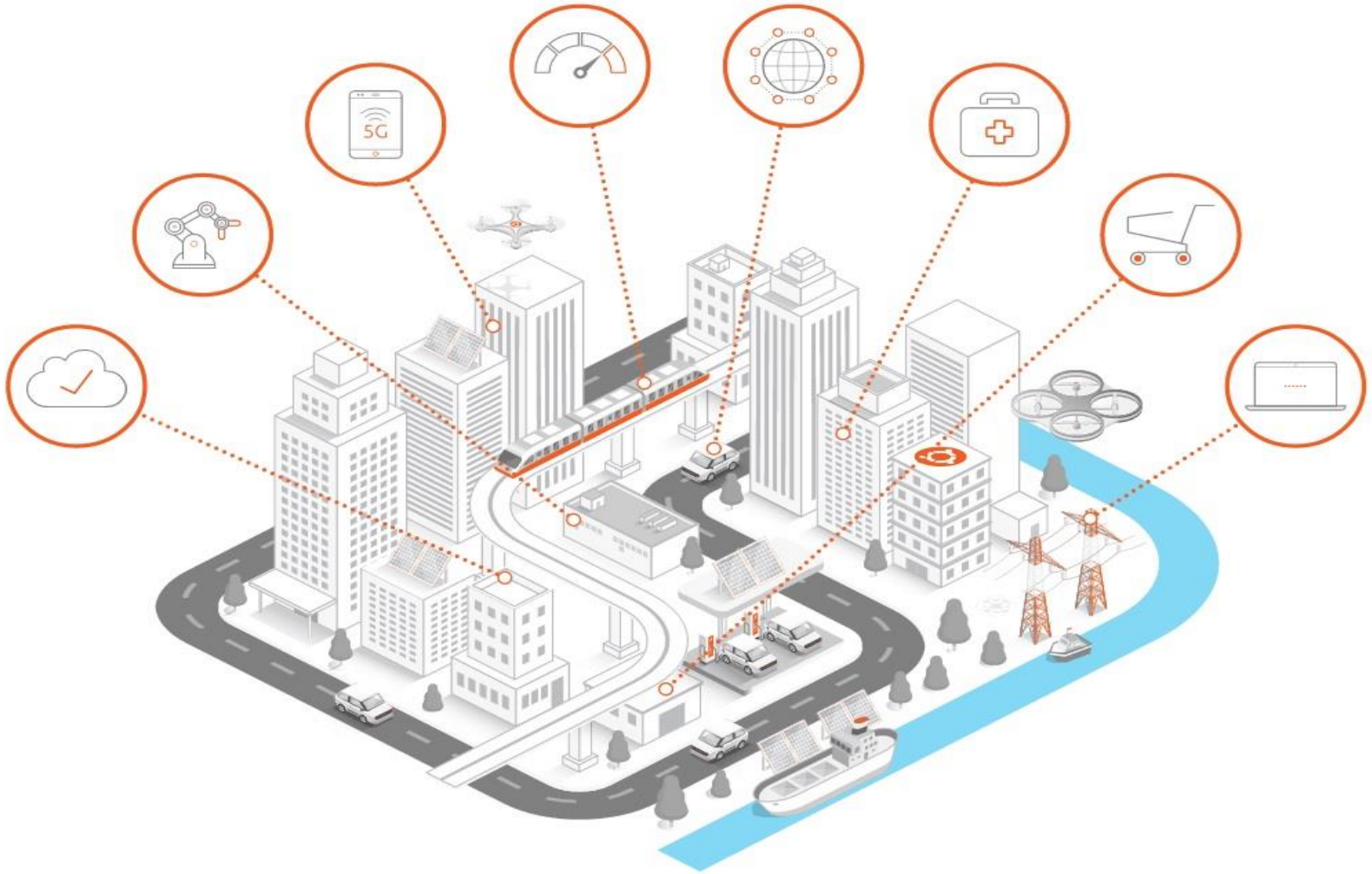
Rogue Endpoints / Edge Devices
A rogue device (endpoint or edge computing device that has been installed on the IoT network without explicit authorization, added by a malicious person) whose data is accepted by the rest of the IoT infrastructure can cause immense damage by rendering the data useless and/or causing unwanted behavior in the whole system.

Compromised Endpoints / Edge Devices
Vulnerable Software on the devices may result in compromised systems. Especially lightweight and price sensitive endpoint devices are extremely hard to patch in a timely manner after a vulnerability has been detected.

Data Leakage
Data from the endpoint- and edge computing devices can hold sensitive information such as personally identifiable information (PII). Leakage of unprotected data can lead to financial and reputational damage.

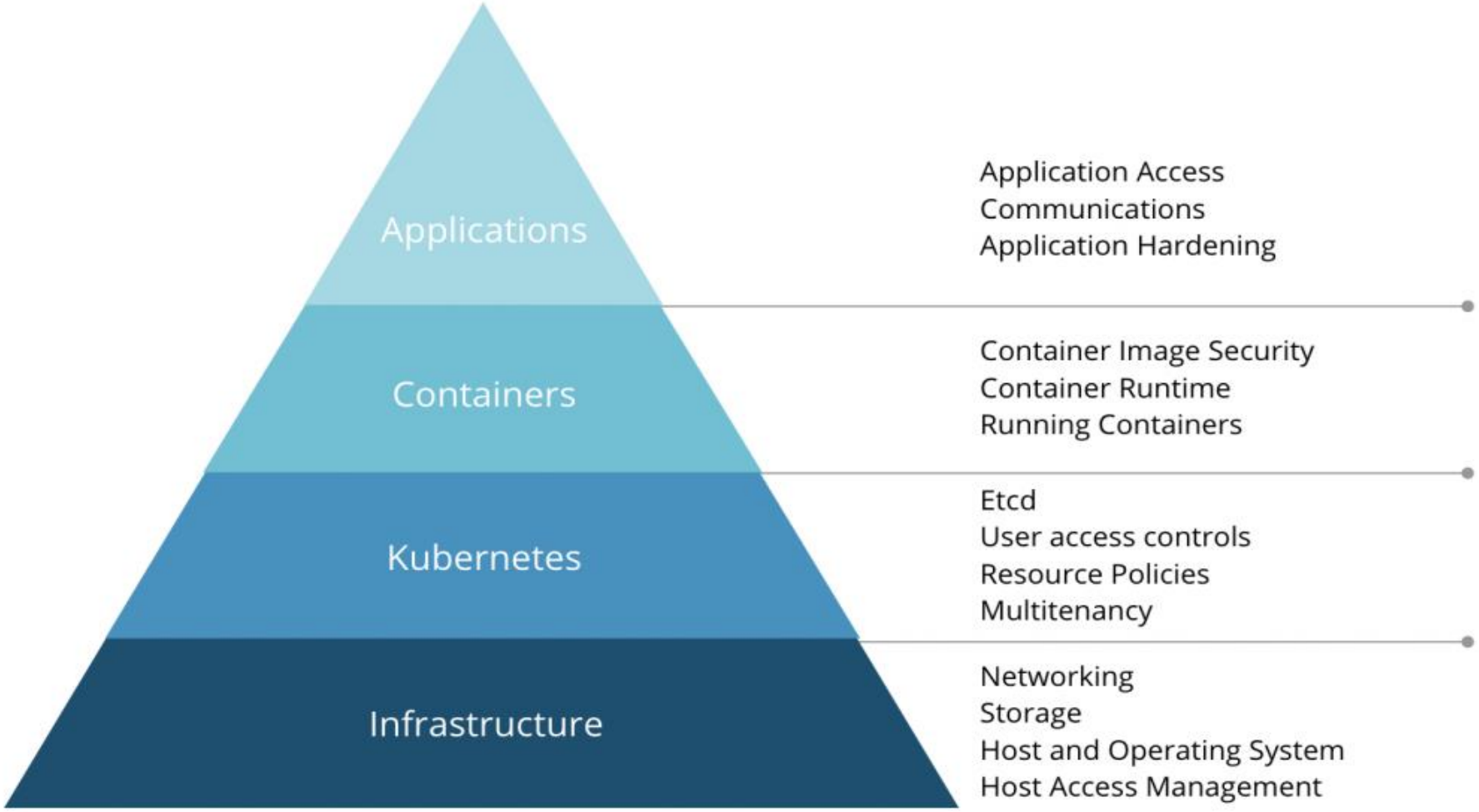


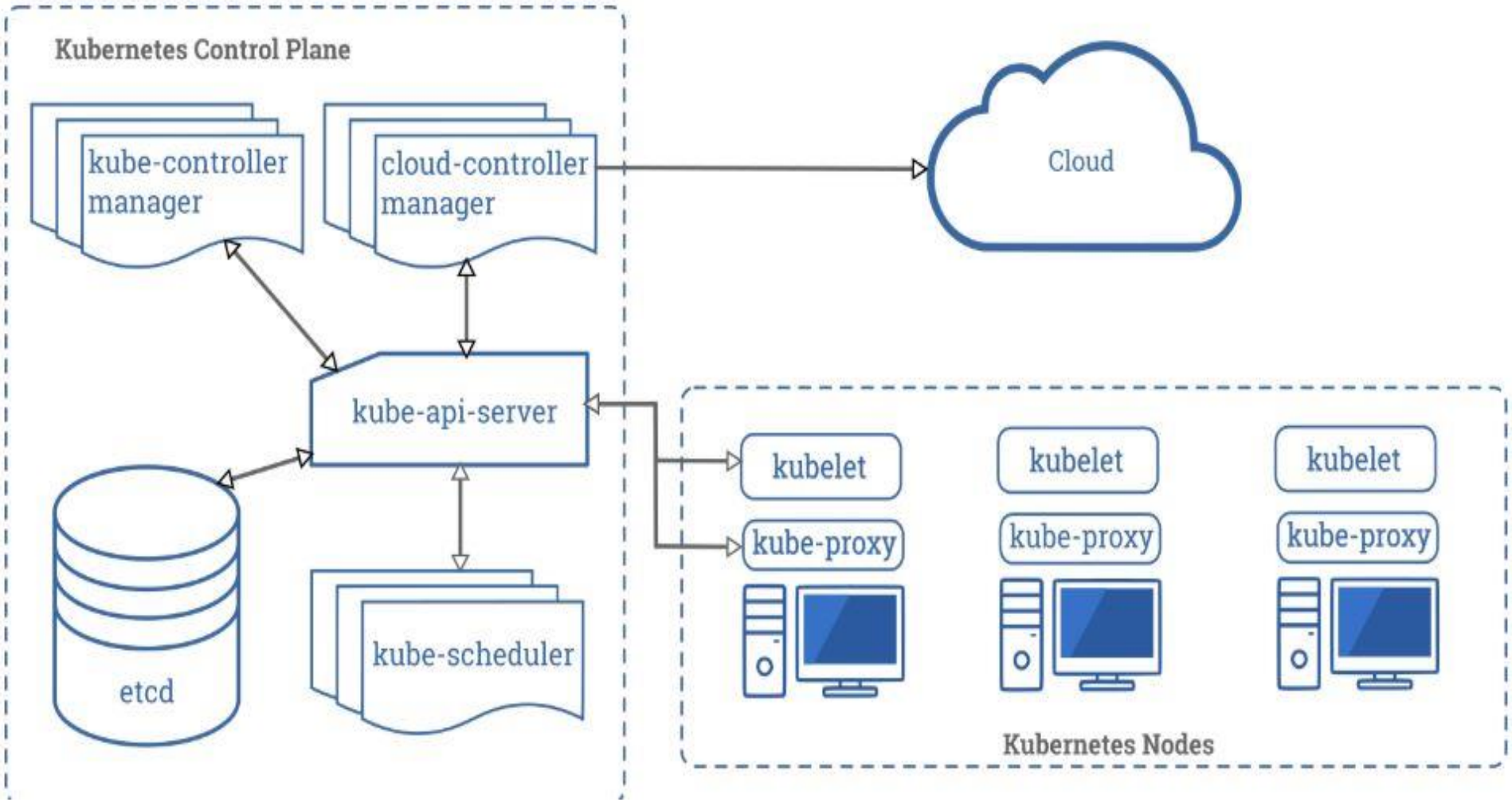
UBUNTU OS for IOT


5G

Attack Surface	Vulnerability
Ecosystem Access Control	• Implicit trust between components • Enrollment security • Lost access procedures
Device Memory	• Cleartext usernames • Cleartext passwords • Third-party credentials
Device Physical Interfaces	• User CLI • Admin CLI • Privilege escalation
Device Web Interface	• SQL Injection • XSS • Weak Passwords
Device Firmware	• Hardcoded credentials • Sensitive information disclosure • Encryption keys

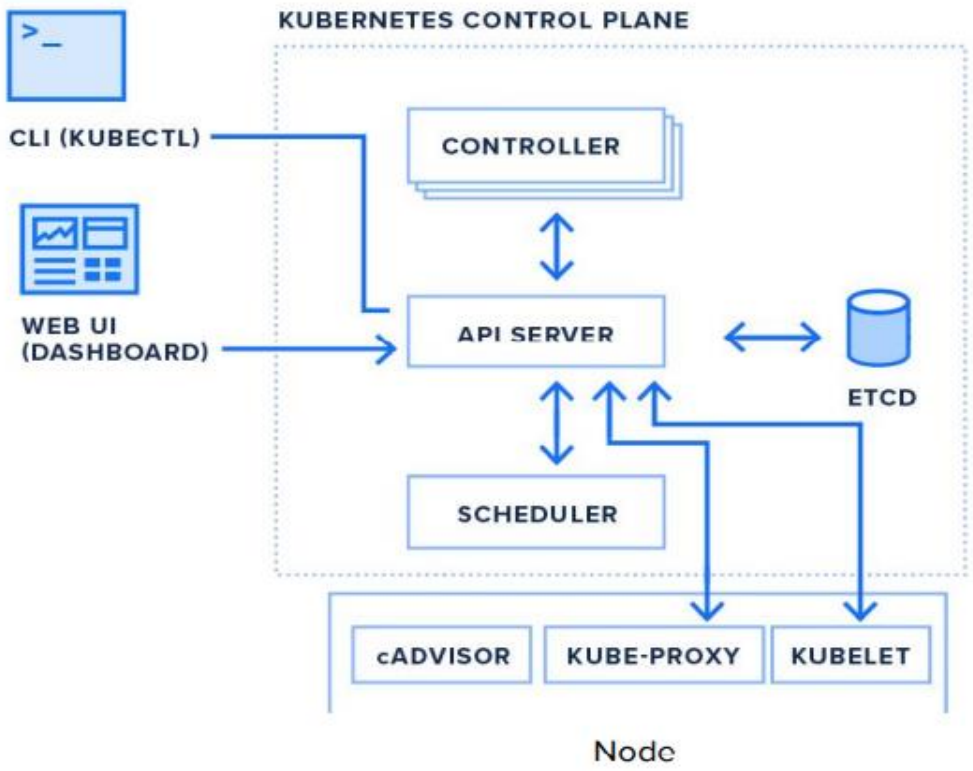
Attack Surface	Vulnerability
Device Network Services	• Denial of Service • Buffer Overflow • Poorly implemented encryption
Administrative Interface	• SQL Injection • Account lockout • Two-factor authentication
Local Data Storage	• Unencrypted data • Data encrypted with discovered keys • Lack of data integrity checks
Cloud Web Interface	• SQL Injection • Weak passwords • Username enumeration
Third-party Backend APIs	• Unencrypted PII sent • Device information leaked • Location leaked


Applications
Containers
Kubernetes
Infrastructure
Application Access
Communications
Application Hardening
Container Image Security
Container Runtime
Running Containers
Etcd
User access controls
Resource Policies
Multitenancy
Networking
Storage
Host and Operating System
Host Access Management


Kubernetes Control Plane
kube-controller manager
cloud-controller manager
Cloud
kube-api-server
etcd
kube-scheduler
kubelet
kube-proxy
kubelet
kube-proxy
kubelet
kube-proxy
Kubernetes Nodes

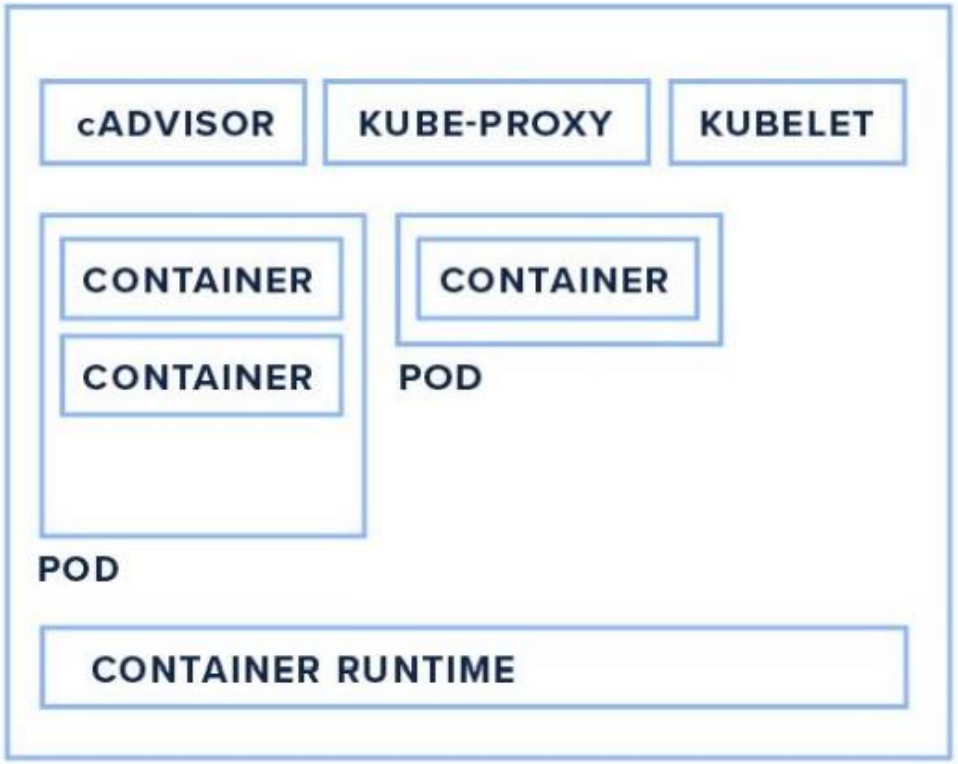
Kubernetes Architecture

- Control Plane
  - API server
  - Scheduler
  - Controllers
    - Kubernetes
    - Cloud
  - Etcd



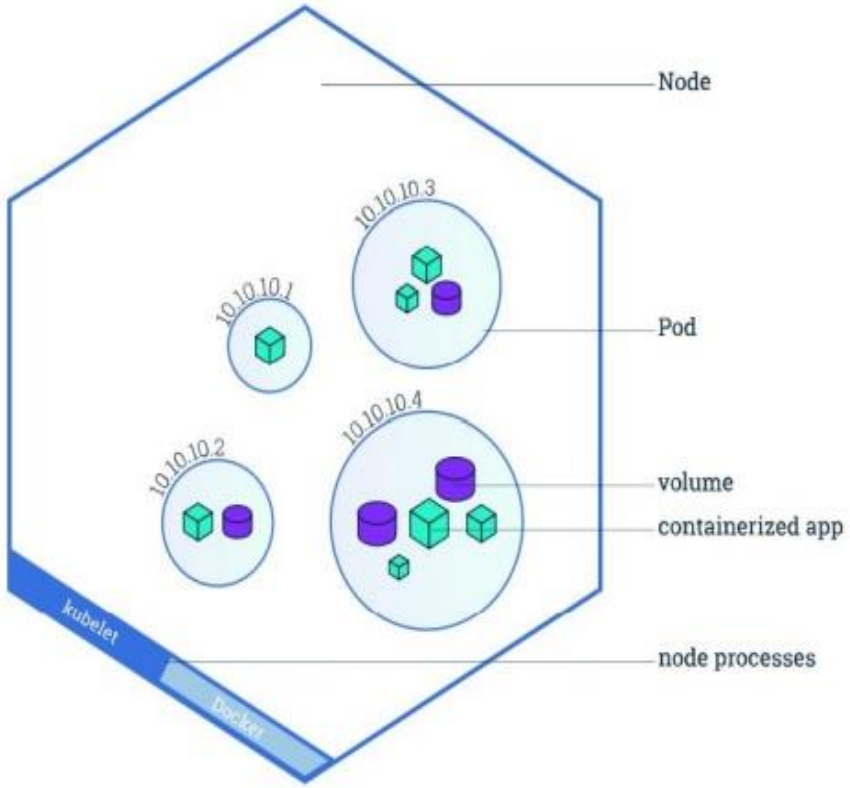
Kubernetes Architecture

- Nodes
  - Kubelet
  - Kube-proxy
  - cAdvisor
  - Container runtime



Pods

- Fundamental Kubernetes work unit
- Can run one or more containers
  - Why more than one?
- Pod containers share resources
  - Storage
  - Network (localhost)
  - Always run on the same Node



Kubernetes Security Checklist and Requirements

- Authentication. ...
- Authorization. ...
- Secure work with secrets. ...
- Cluster Configuration Security. ...
- Audit and Logging. ...
- Secure OS configuration. ...
- Network Security. ...
- Secure configuration of workloads.

Calico Cloud enables fine-grained, zero-trust workload access controls between your microservices and external databases, cloud services, APIs, and other applications. It also prevents the lateral movement of threats with identity-aware segmentation that works across all of your workload environments, including hosts, VMs, Kubernetes components, and services. Finally, Calico Cloud provides workload-based security controls for runtime intrusion detection and prevention, protection from DDoS attacks, deep packet inspection (DPI) and an envoy-based web application firewall (WAF) capability.

- Data plane - Linux eBPF
- Kubernetes Network Policy
- High-performance scalable pod networking
- Multi and Hybrid Cloud
- Data plane - Linux iptables
- Policy for Hosts, VMs, and Kubernetes
- Advanced IP address management
- On-premises
- Data plane - Windows
- Security Policy for Kubernetes Services
- Direct infrastructure peering without the overlay
- Data-in-transit encryption
- Data plane - VPP
- Security policy for high-connection workloads
- Kubernetes Networking


thank you
danke
謝謝
ngiyabonga
teşekkür ederim
gracias
tapadh leat
спасибо
рахмат
Баярлалаа
bedankt
dziękuję
obrigado
merci
go raibh maith agat
mochchakkeram
sukriya
kop khun krap
terima kasih
arigatō
dakujem
мерси
grazie
takk
taiku
sagolun
hvala
mauruuru
dank je
misaotra
blagodaram
matondo
paldies
grazzi
mahalo
хвала
asante
manana
obrigada
murakoze
tenki
djiere dieuf
mamnun
chnorakaloutioun
gracies
sulpay
tack
welalin
barka
mersi
spas
kiitos
dankie
dhanyavad
nandri
nanni
bayarlalaa
gracie
koszonom
akun
dankon
aciu
enkosi
sobodi
dèkuji
mesi
didi madloba
najis tuke
kam sah hamnida
rahmat
tanemirt
rahmet
diolch
dhanyavadagalu
shukriya
merce
trugarez
xiexie
감사합니다
ありがとう
তোমাকে ধন্যবাদ
ευχαριστώ