A DevOps Approach for Extending Cloud Computing to the Edge

Grace A. Lewis

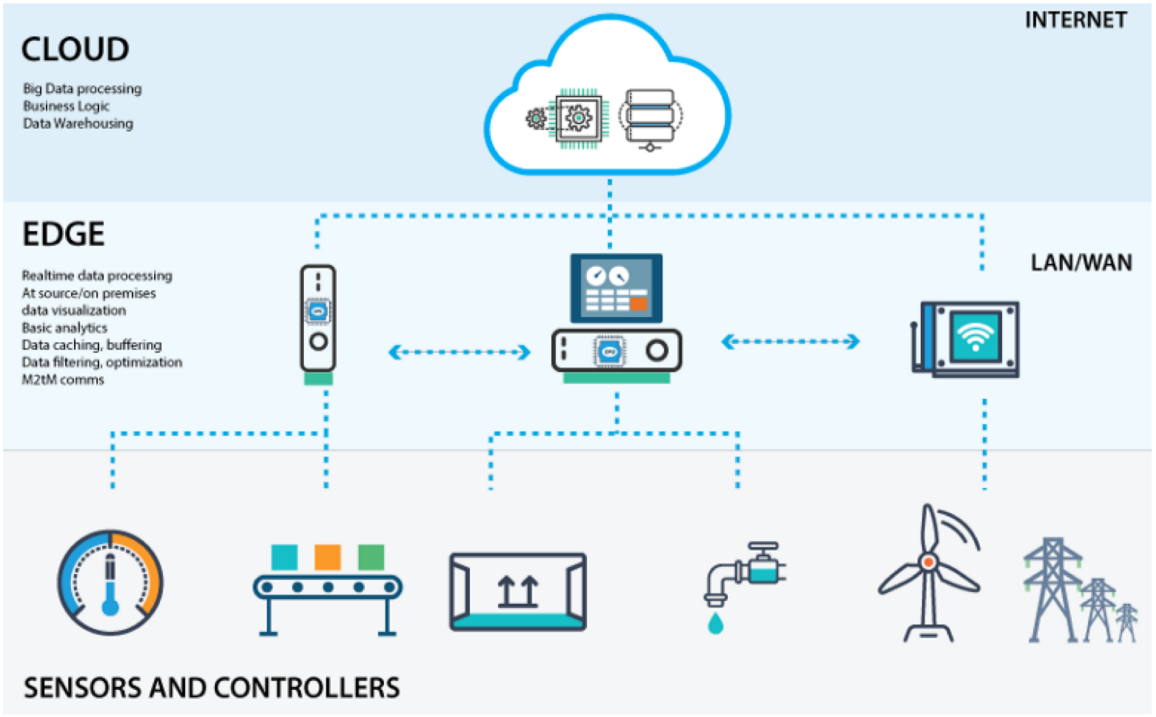
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM18-1079

Background: Edge Computing

Model in which applications, data, and computing power are pushed to the logical extremes of a network — closer to mobile devices, end users, and more recently IoT devices



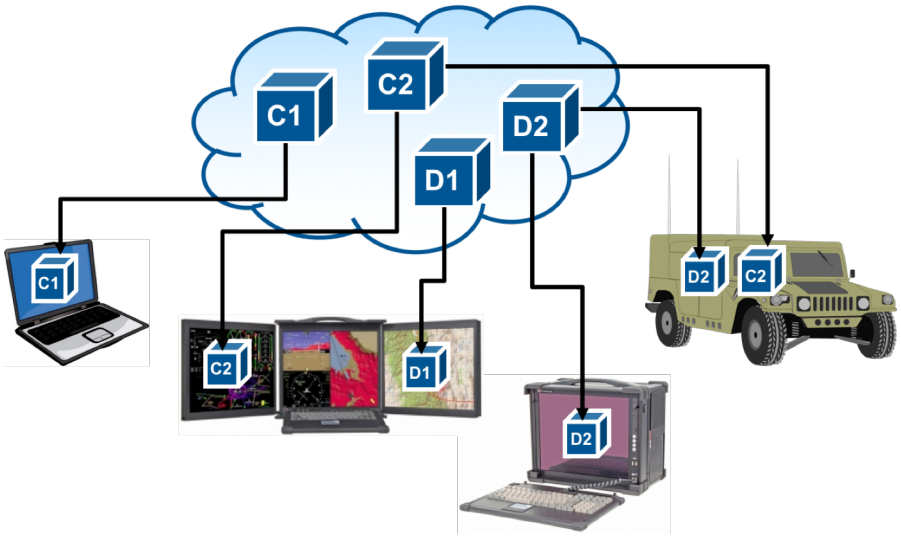
Source: OAS

Motivation: Not Everyone is Connected to the Cloud

Soldiers, first responders, and medic operating in the field require access to cloud resources to perform their missions. However ...

- They operate in environments that have disconnected-intermittent-limited (DIL) connectivity
- Access to computation and data in the cloud is not always possible

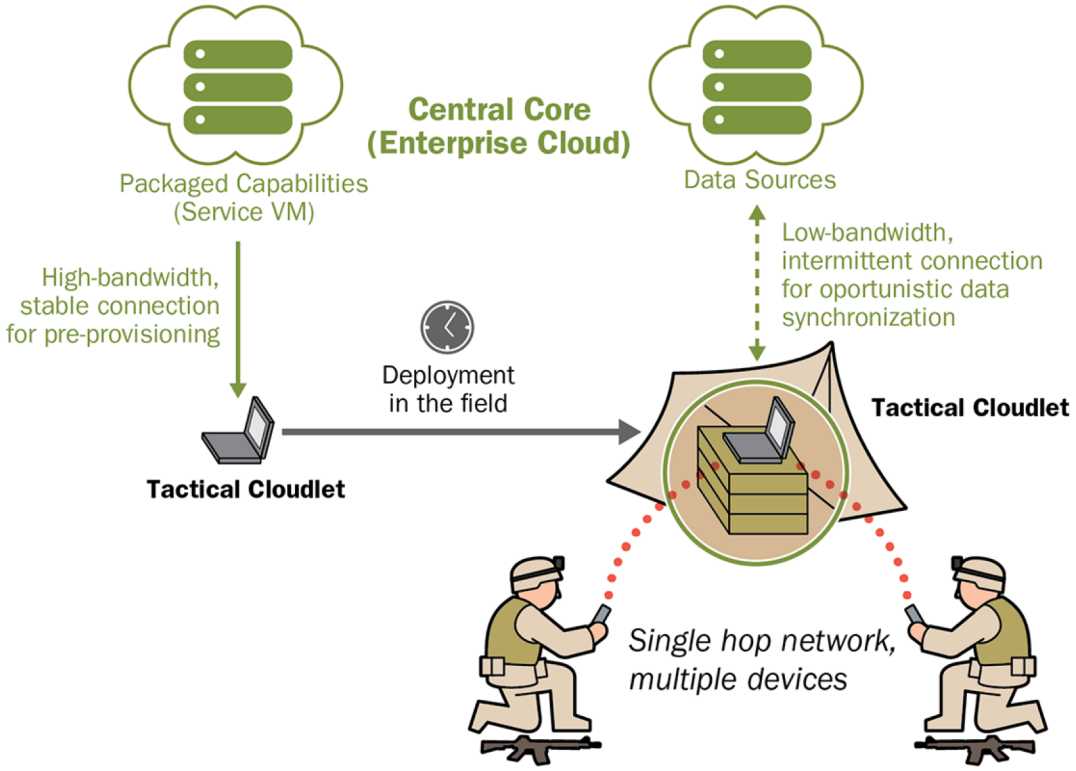
Technical challenge: “Carve out” a piece of the cloud and make it accessible to personnel operating in these environments in a secure, reliable, and timely manner



Tactical Cloudlets

Forward-deployed, **discoverable**, virtual machine (VM) based computing nodes that can be hosted on vehicles or other platforms to provide

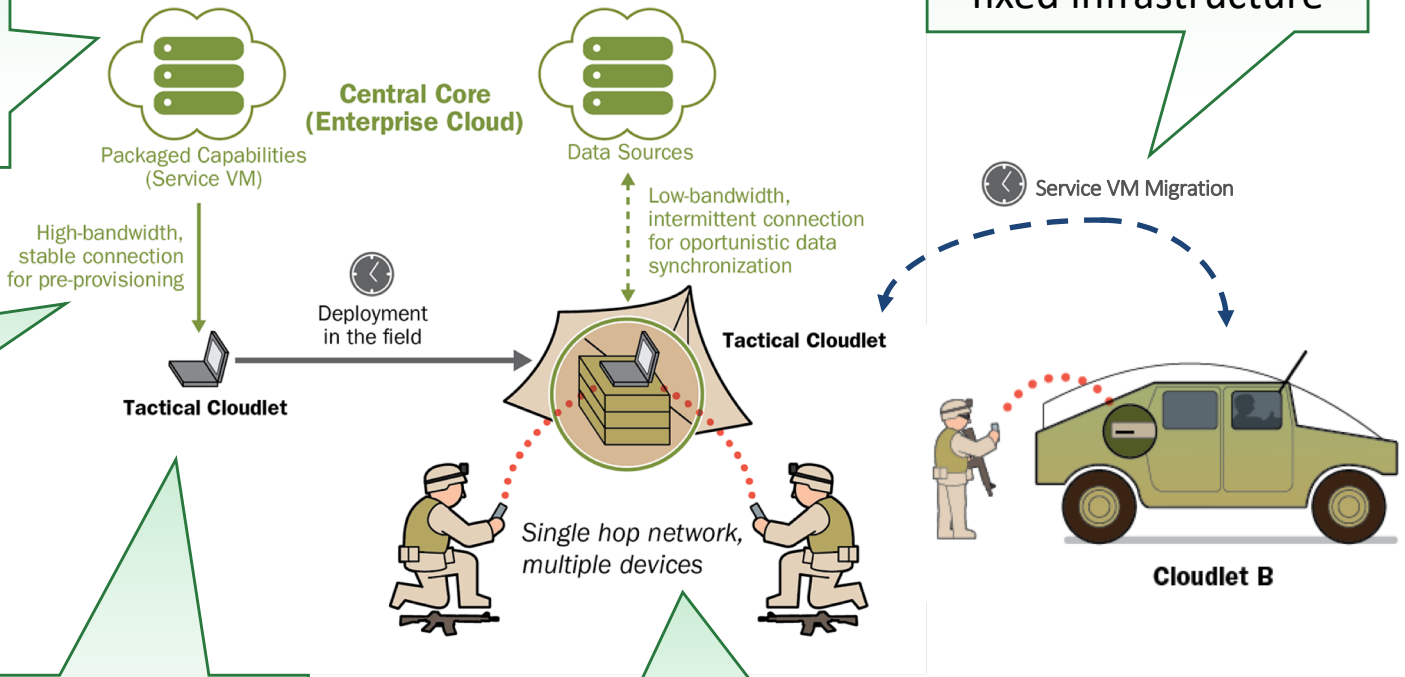
- infrastructure to offload computation
- forward-data-staging for a mission
- data filtering to remove unnecessary data from streams intended for mobile users
- collection points for data heading for enterprise repositories



Tactical Cloudlet Features

Standard Packaging of Service VMs to support ease of provisioning, scalability, and reuse

Secure Service VM Migration enables mobility and reintegration to a fixed infrastructure



Pre-Provisioned Cloudlets with App Store to support disconnected operations

Cloudlet Management Component provides console-like capabilities and credential management

Secure Key Generation and Exchange for establishing trust between cloudlets and mobile clients

Limitations for Operational Use

Cloudlet provisioning is currently a very manual process

- Service VMs have to be manually added
- Network and security configuration is a long and manual process

Implementation is not ATO-ready

- ATO is Authority to Operate
- When a product receives ATO it means that it has implemented all required security controls

Next Step: A DevOps Approach for Extending Cloud Computing to the Edge

Automated ATO-Ready Cloudlet Provisioning (Static)

- Use DevOps concepts and tools to develop mechanisms for cloudlets to be quickly provisioned with the services and security controls necessary to operate in the field

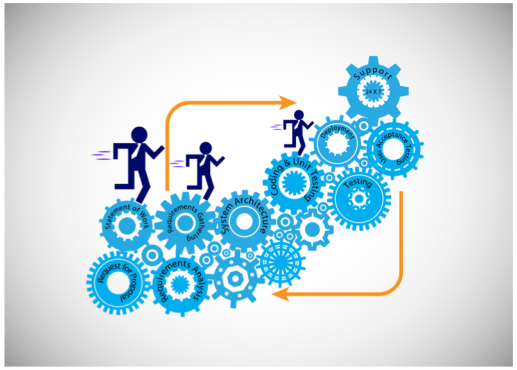
Automated ATO-Ready Cloudlet Provisioning (Dynamic)

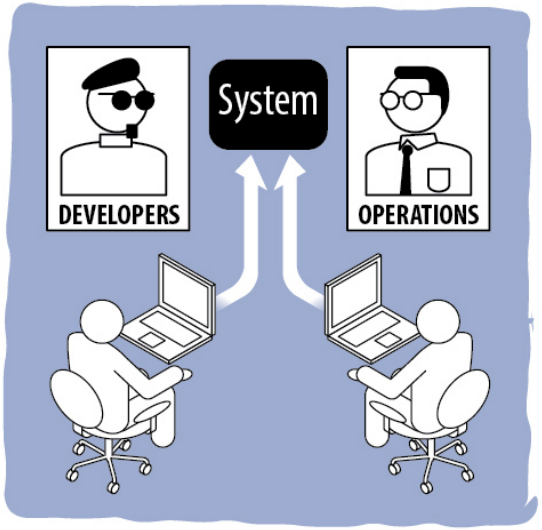
- Extend static methods for automated ATO-ready cloudlet provisioning with capabilities to dynamically provision, re-provision, or decommission cloudlets

DevOps

Set of principles and practices that emphasize collaboration and communication between software development and IT operations teams and tools

- Collaboration: between project team roles
- Infrastructure as Code: all assets are versioned, scripted, and shared where possible
- Automation: deployment, testing, provisioning, any manual or human-error-prone process
- Monitoring: any metric in the development or operational spaces that can inform priorities, direction, and policy



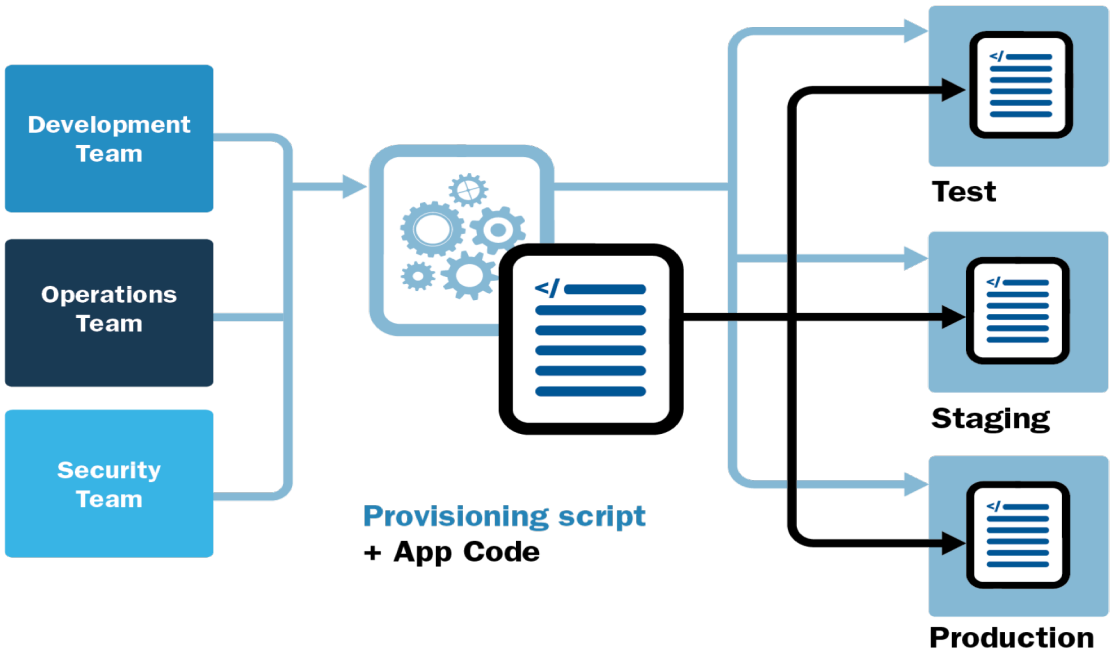


Source: Hasan Yasar. DevOps in Practice Workshop. 2018.

Infrastructure as Code (IaC)

IaC is a program that creates infrastructure

- Creates VMs
- Provisions VMs or physical hardware with specific dependencies, configurations, networking

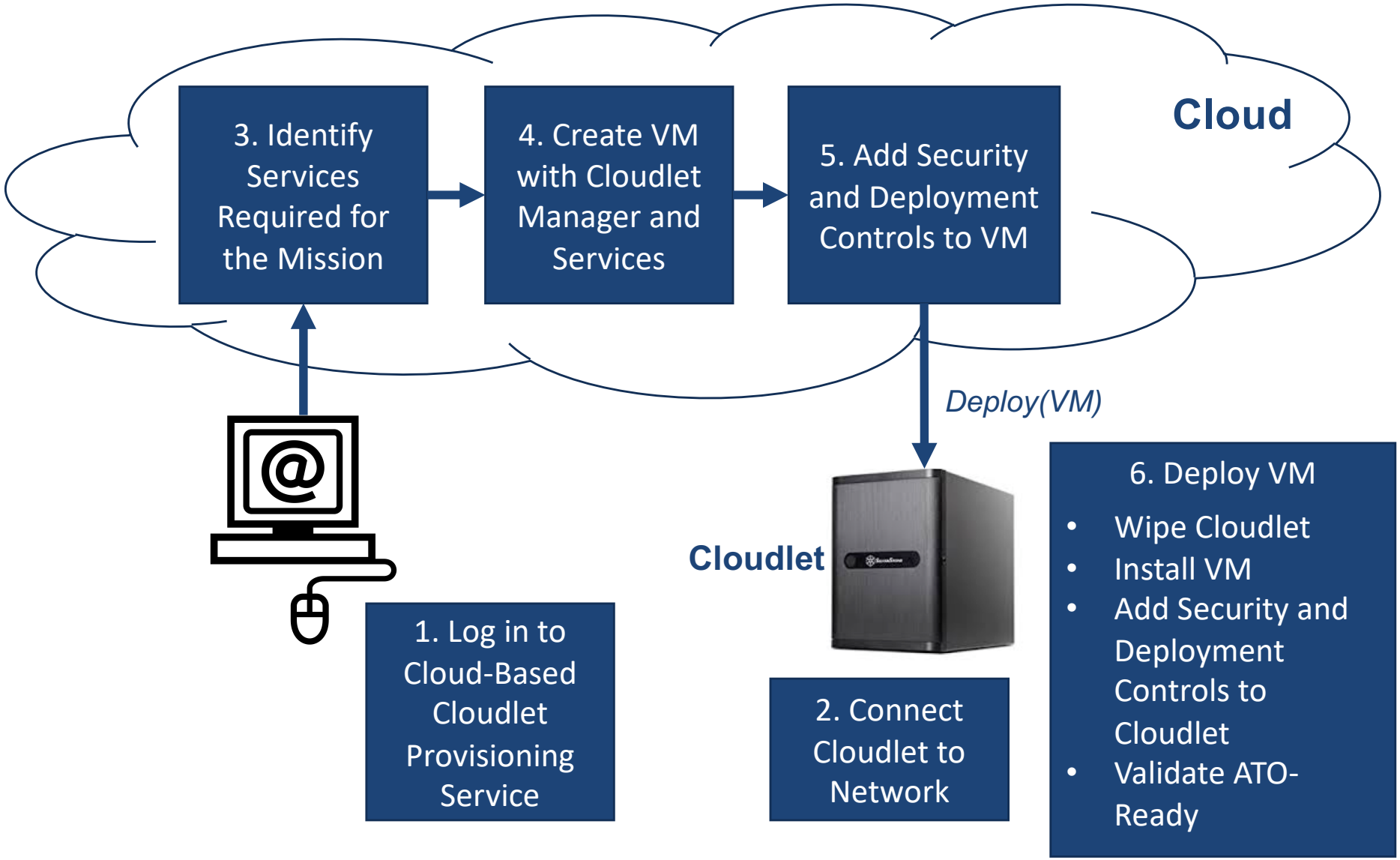


Source: Hasan Yasar. DevOps in Practice Workshop. 2018.

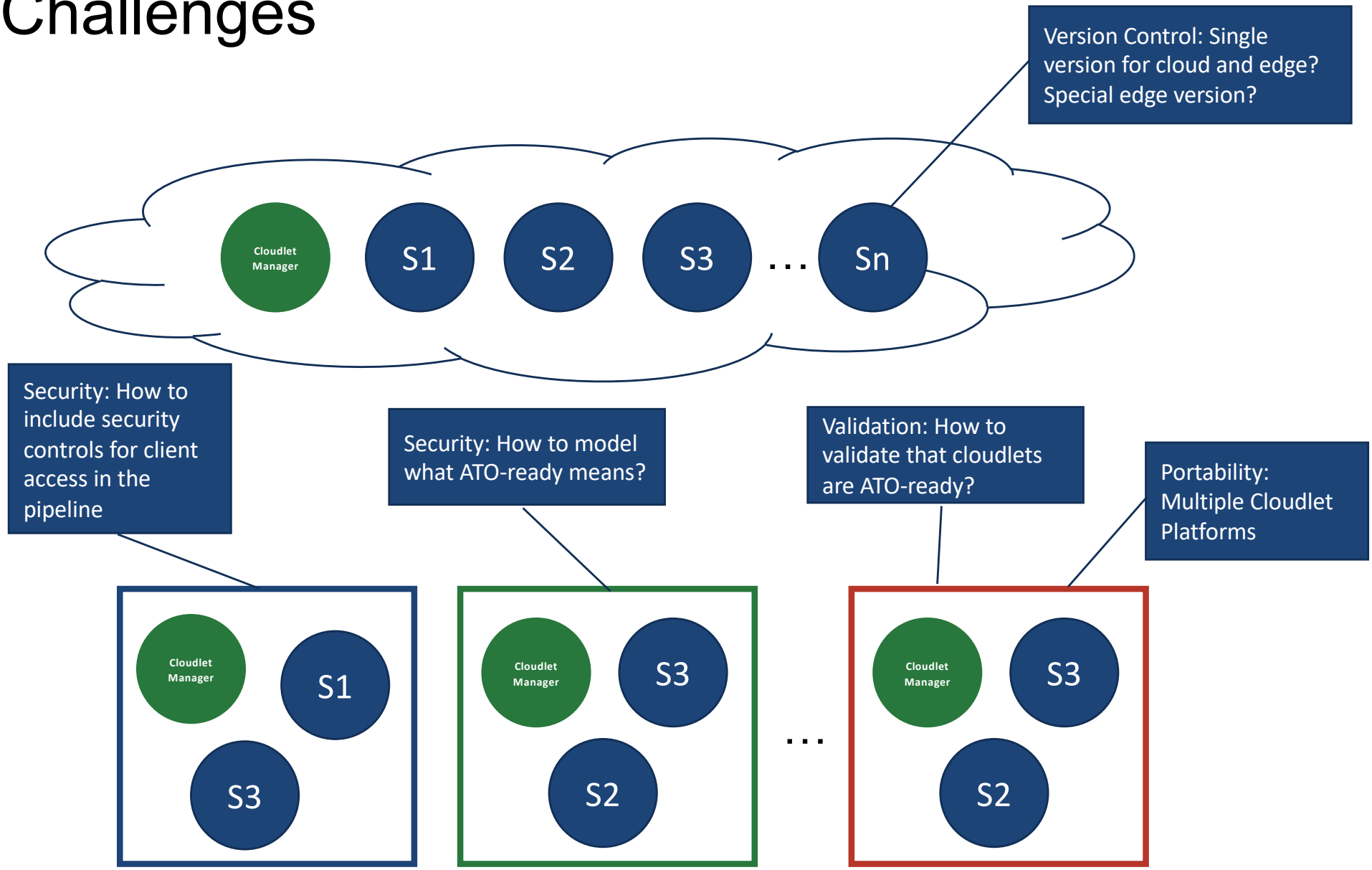
Automated ATO-Ready Cloudlet Provisioning (Static)

- Develop methods and tools for ATO-ready deployment at the edge that can securely push cloud capabilities to the edge
  - Edge capabilities are packaged as lightweight microservices
  - Cloudlets are set up pre-mission with required services
  - Security controls are built into the provisioning and deployment toolchain
- Extend methodology and toolchain for automated ATO-ready provisioning of mobile devices and sensors that interact with cloudlets at the edge

Vision



Challenges



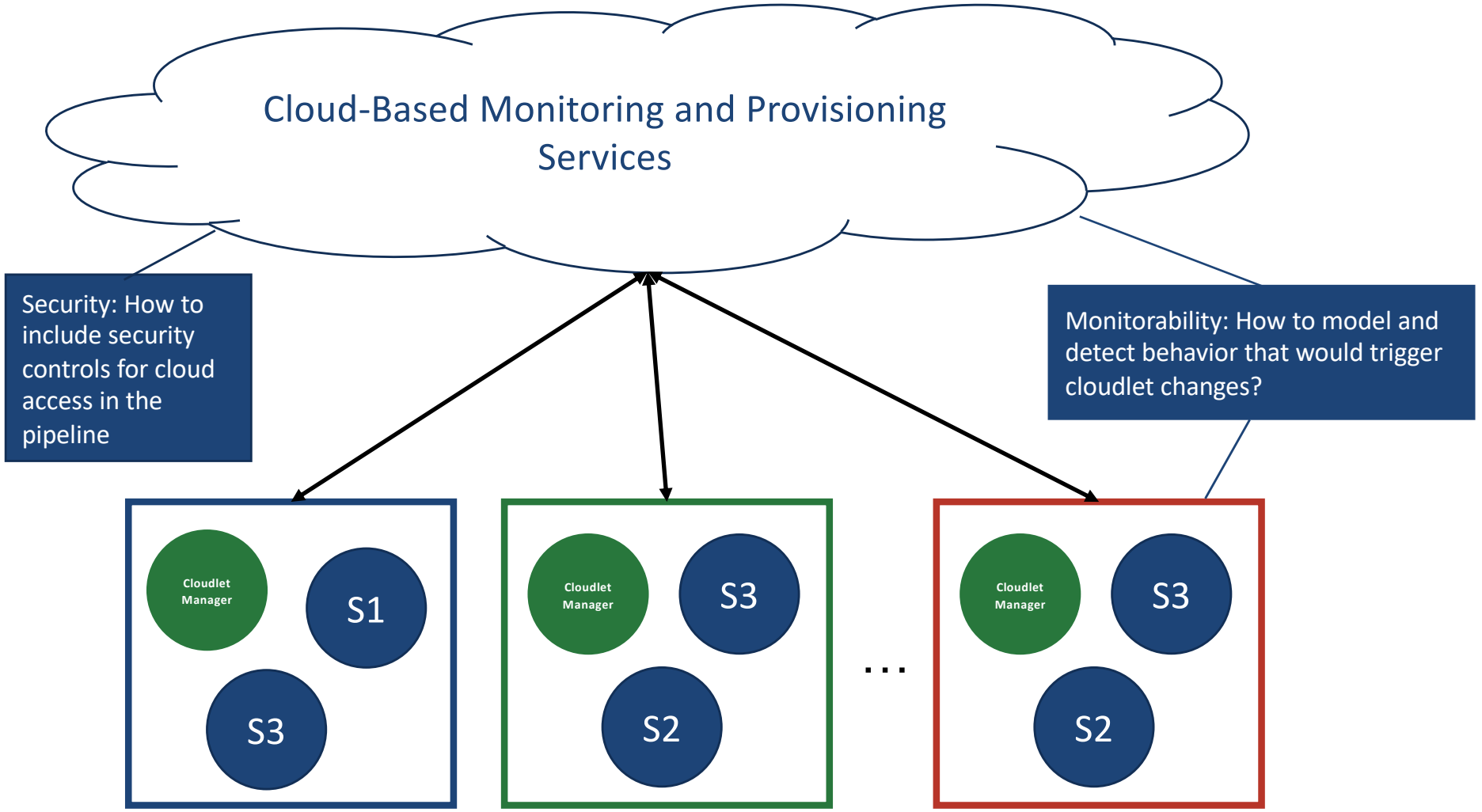
Automated ATO-Ready Cloudlet Provisioning (Dynamic)

Motivation: Not all edge environments are disconnected

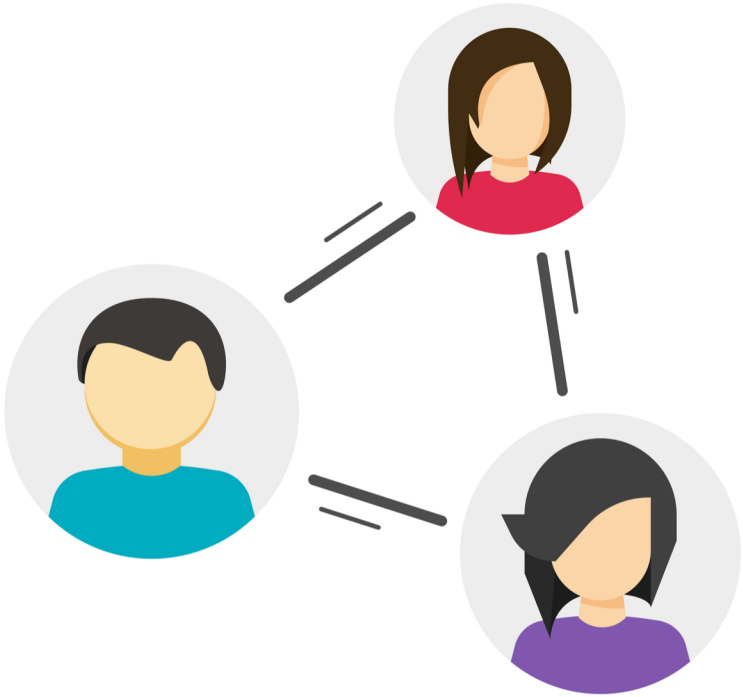
Approach

- Extend static methods for automated ATO-ready cloudlet provisioning with capabilities to dynamically re-provision or decommission cloudlets based on
  - Mission changes
  - Cloudlet (sensor) tasking
  - Suspicious behavior
- Develop and incorporate AI/ML-based analytics to more proactively react to changes

Additional Challenges



Interested in Collaboration?



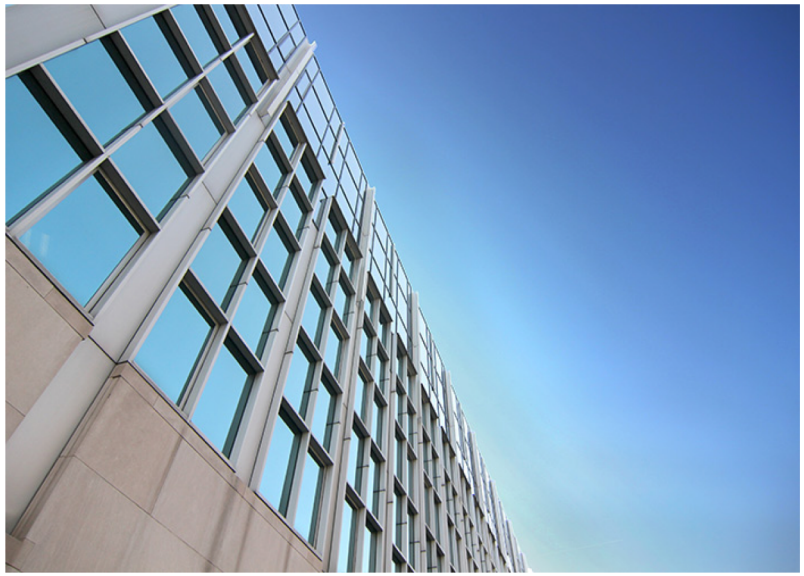
Contact Information

Principal Investigator

Grace A. Lewis
Principal Researcher (SSD/TTG)
Telephone: +1 412.268.5851
Email: glewis@sei.cmu.edu
WWW: http://www.sei.cmu.edu/staff/glewis/

Team

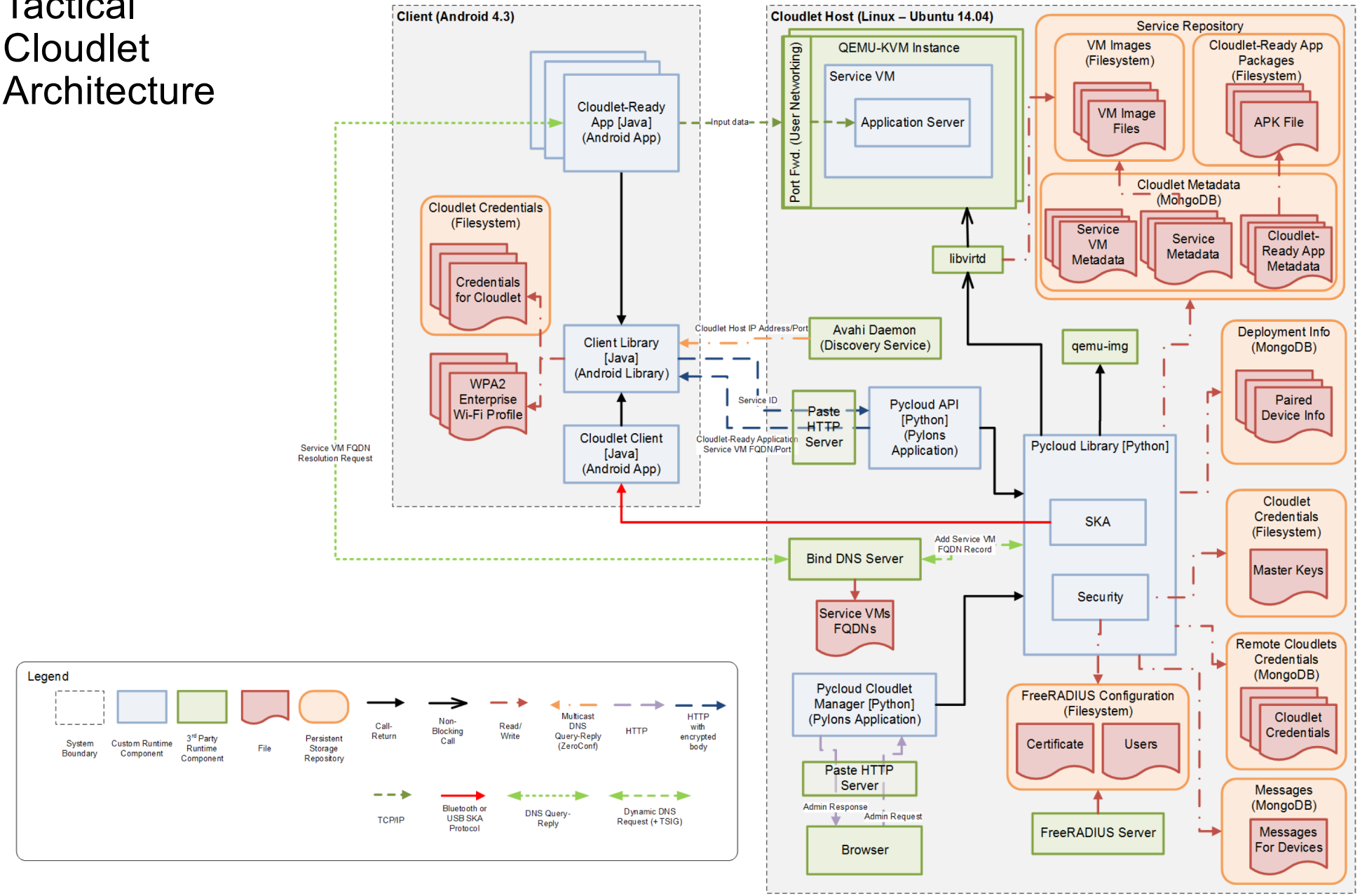
Sebastían Echeverría (SSD/TTG)
Chris Grabowski (SSD/TTG)
Dan Klinedinst (CERT/VUL)
Keegan Williams (SSD/TTG)



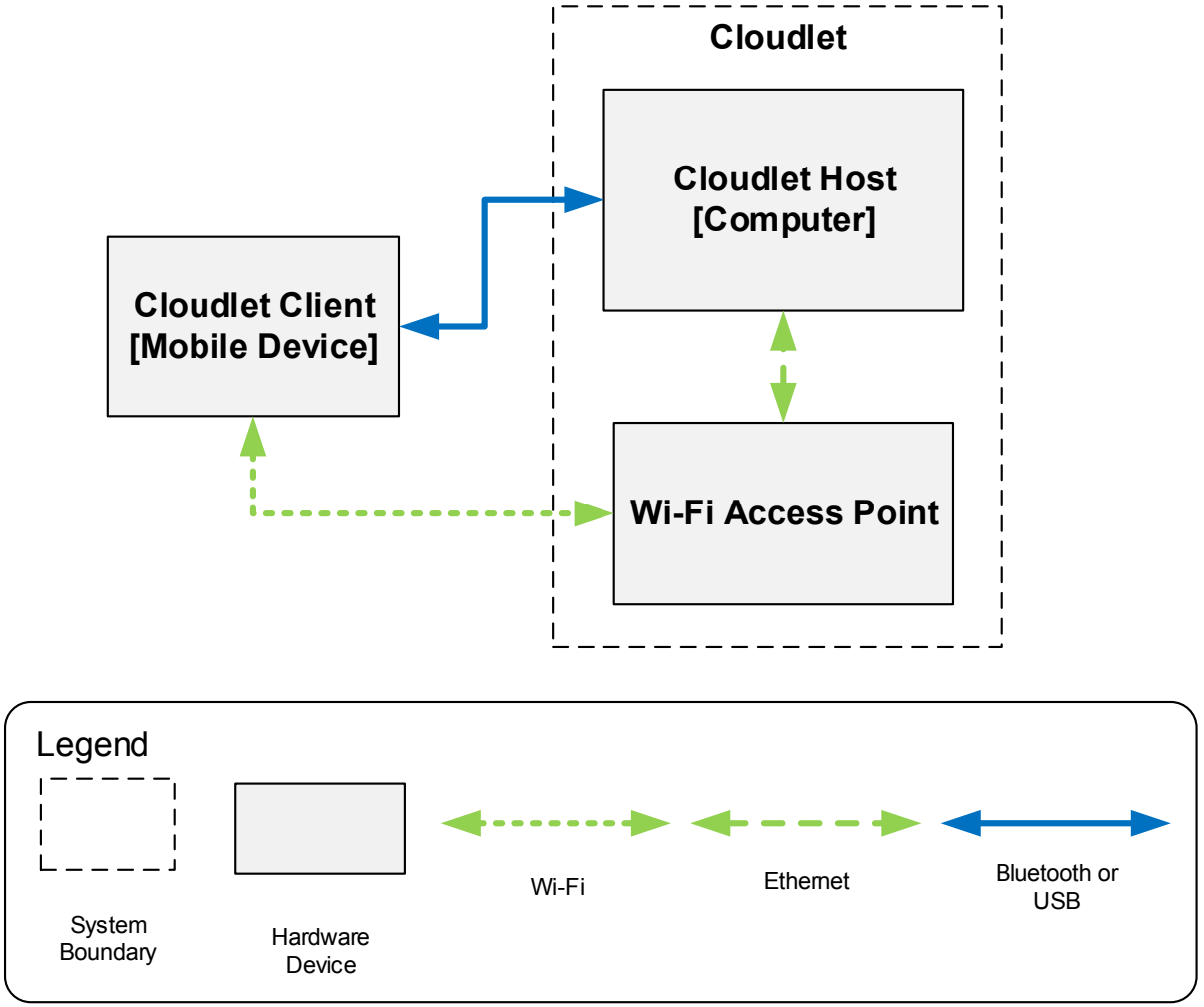
Tactical Cloudlets software available on GitHub as KD-Cloudlet
https://github.com/SEI-AMS/pycloud

Backup Slides

Tactical Cloudlet Architecture



Tactical Cloudlet Physical View



Tactical Cloudlets Features

Edge Characteristics Capabilities/Features	Intermittent cloudlet-enterprise connectivity	Mobility	Limited battery power	Dynamic missions	Limited technical skills in the field	Potentially hostile environments
System Requirements	*Disconnected operations*	*Quick response time*	*Low energy consumption*	*Ease of re-deployment*	*Ease of deployment*	*Trusted identities*
Pre-Provisioned Cloudlets with App Store	X	X	X	X	X	
Standard Packaging of Service VMs				X	X	
Cloudlet Management Component				X	X	
Cloudlet Handoff/Migration		X		X		X
Secure Key Generation and Exchange	X					X

Pre-Provisioned Cloudlets with App Store

Applications statically partitioned into a client and server

- Very thin client runs on mobile device (App)
- Computation-intensive server runs on cloudlet (Service VM)

Capabilities as services

- Service VM provides a self-contained capability and exposes a simple interface
- Service VM metadata includes the client app for the capability

Virtual machines as service containers

- VMs can be started and stopped as needed based on number of active users therefore providing scalability and elasticity
- Also enables legacy system reuse

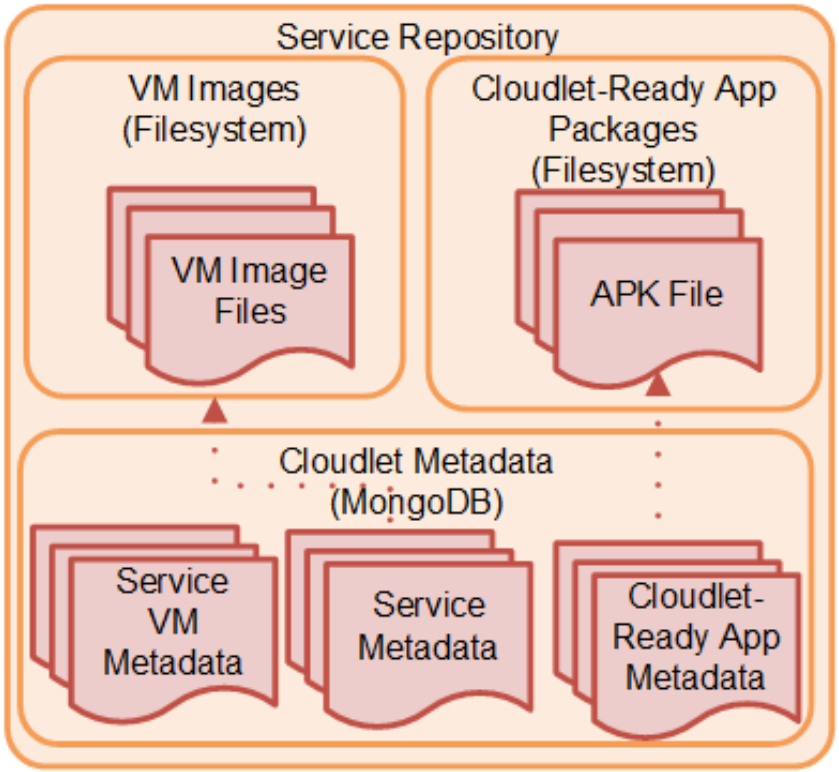
Request-Response interactions between clients and cloudlets

- Enables easy detection of failed communication between mobile devices and cloudlets
- Also minimal effect on mobile devices if computation needs to be restarted or migrated

Standard Packaging of Service VMs

Standard format for Service VMs (.csvm) so these can be easily loaded from the cloudlet disk drive, an enterprise Service VM repository, a thumb drive, or a mobile device connected via USB or Bluetooth to the cloudlet

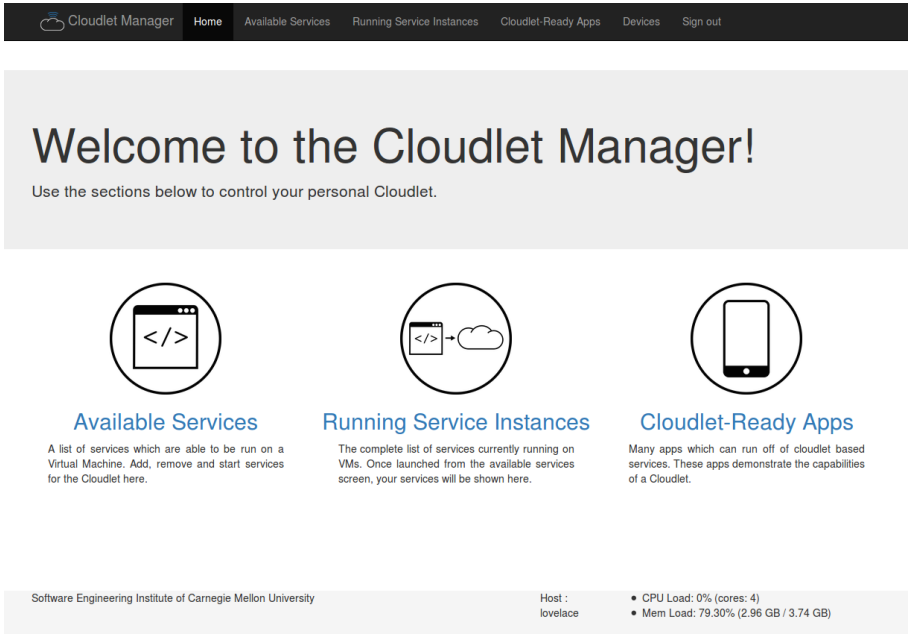
- Service metadata (JSON file): service ID, port, version, description, tags, shared/non-shared, minimum memory, ideal memory
- VM image files — one for the disk image and one for the state/memory image that contain a suspended Service VM

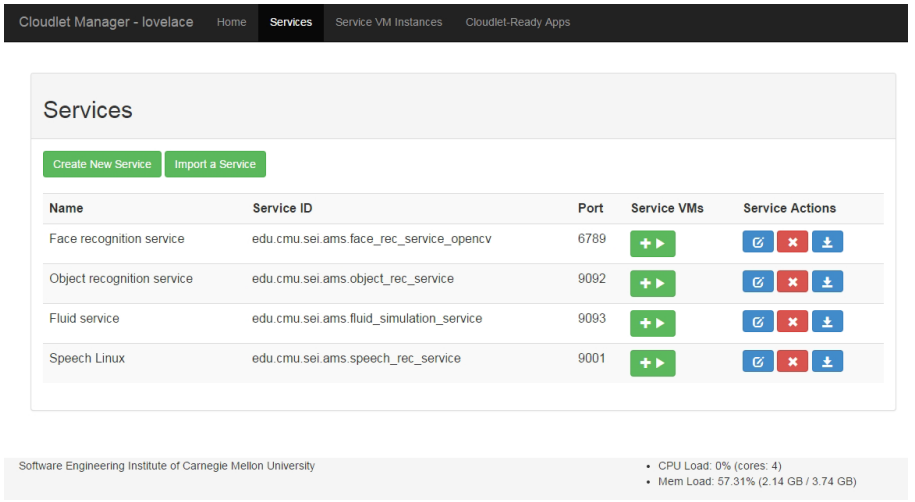


Cloudlet Management Component

Lightweight, web-based interface that enables easy deployment and redeployment of capabilities

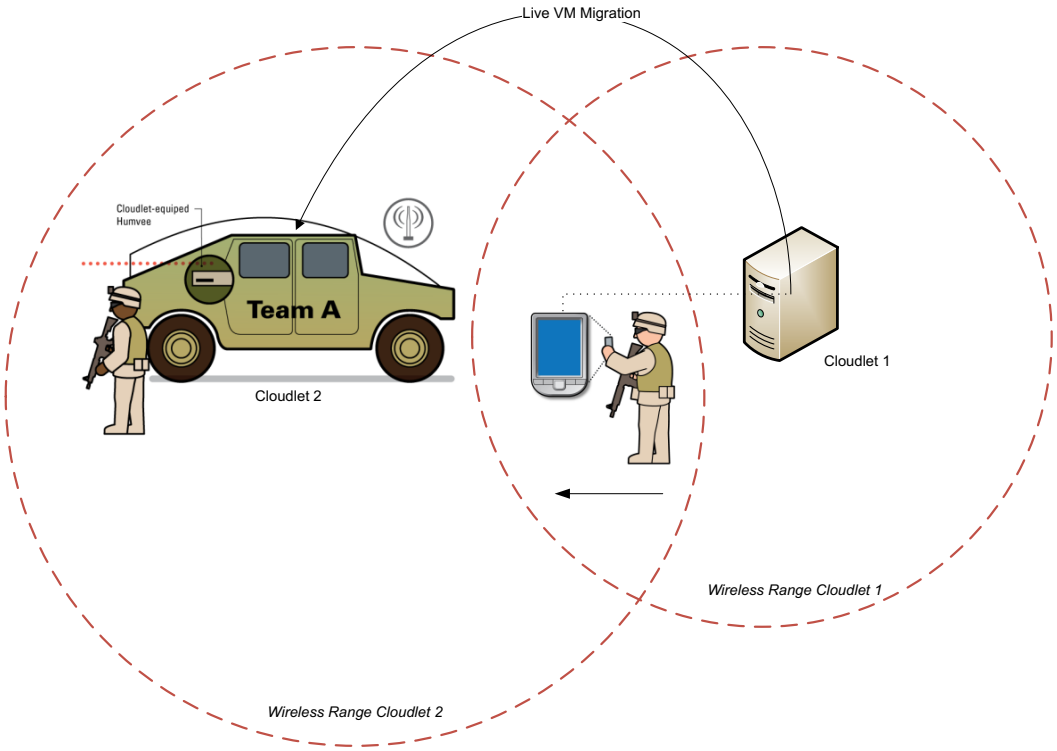
- Service VM creation, edit and deletion
- Service VM import and export
- Service VM Instance start, stop and migration
- Cloudlet-Ready App repository (i.e., app store)
- Credential management





Cloudlet Handoff/Migration

Manual handoff enables scenarios in which a user is migrating capabilities from a fixed cloudlet to a mobile cloudlet to support field operations, as well as reintegration back to the fixed cloudlet



Desire is to support automatic migration based on for example signal strength, load balancing or a more powerful surrogate in proximity

Secure Communications – Validation

Threat modeling

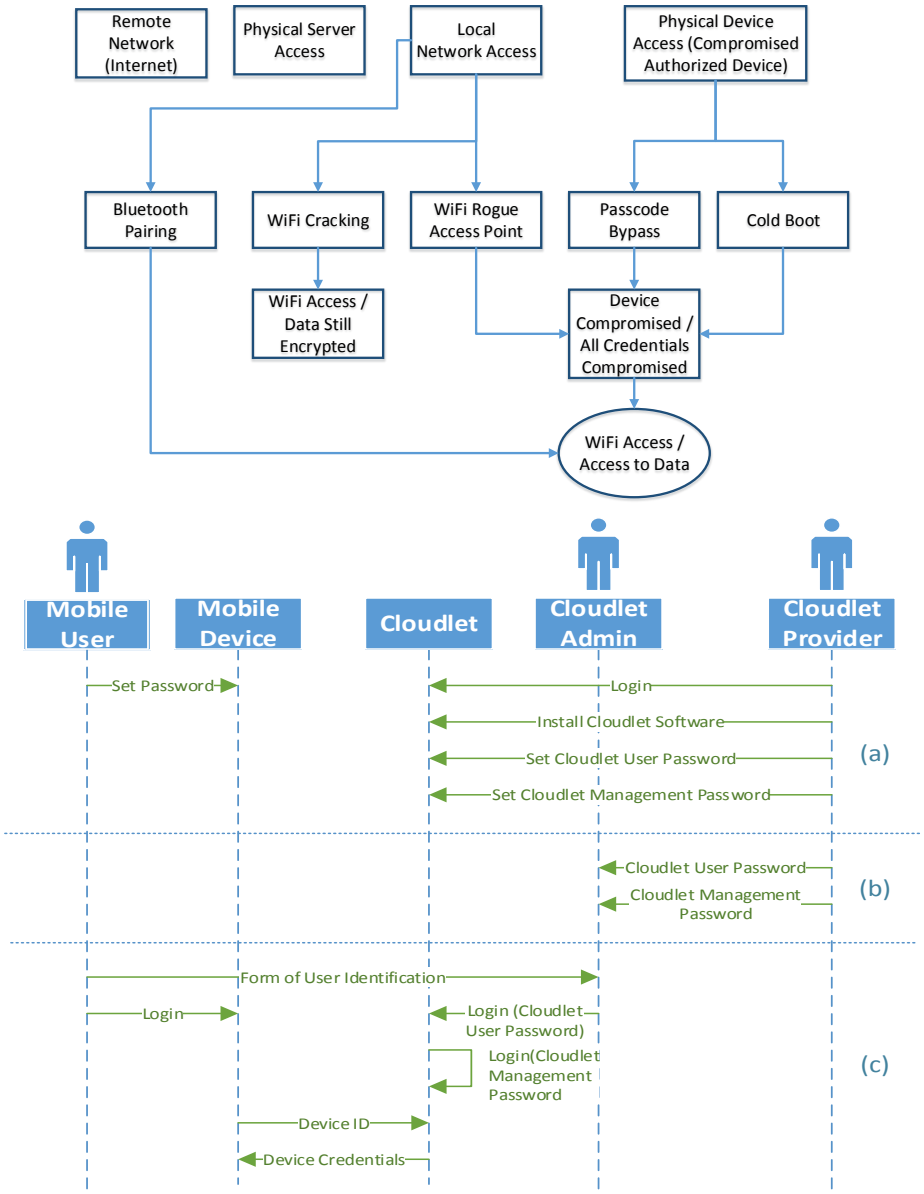
- Identified and prioritized 14 threats
- Solution addresses 12 threats (directly or indirectly)

Vulnerability analysis

- Architectural and technical analysis of possible vulnerabilities using a simple attack tree based on the threat model

Ceremony analysis

- Ceremonies include all protocols, applications with a user interface, and security provisioning workflows — nothing is out of band



Secure Key Generation and Exchange

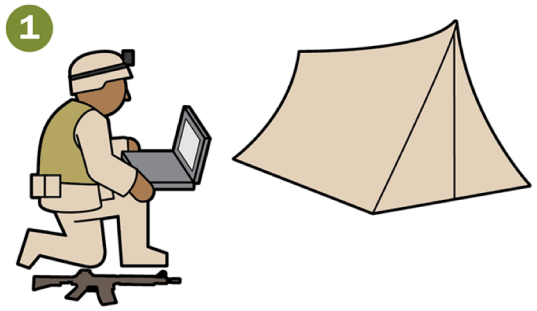
Motivation

- Common solution for establishing trust is to create and share credentials in advance, and then use an online trusted authority for validation
- However, characteristics of tactical environments do not consistently provide access to a credential repository or online authority

Solution Requirements

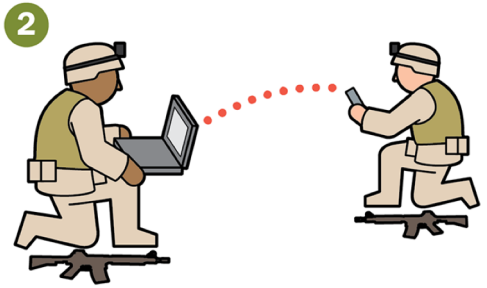
- Cannot require network connectivity to a third party for credential generation or validation
- Cannot place any specific security requirements on hardware
- Cannot require pre-provisioning of credentials on the mobile devices
- Must address the threats of a tactical environment

Secure Communications



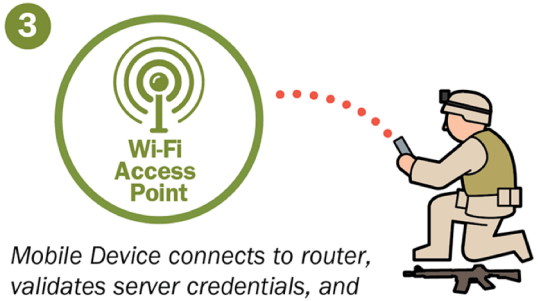
Admin logs into the Cloudlet Manager to start the Bootstrapping process

Bootstrapping
- Generation of *Cloudlet Credentials* using IBE (Identity-Based Encryption)
- Setup of *RADIUS Server* with *Cloudlet Credentials*



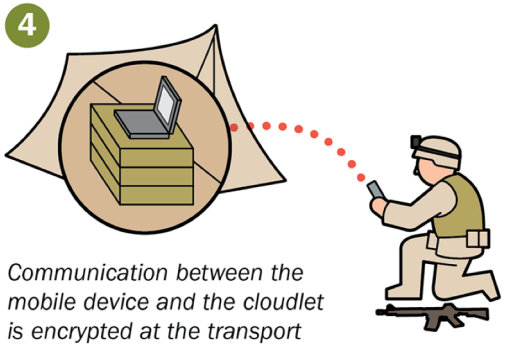
User connects mobile device to the cloudlet, and upon visual confirmation the admin starts the pairing process

Pairing
- Generation of *Device Credentials* using IBE
- Transfer to device using Bluetooth or USB, plus visual confirmation
- Transfer to *RADIUS Server*



Mobile Device connects to router, validates server credentials, and authenticates with RADIUS server

Wi-Fi Authentication
RADIUS Server implements Wi-Fi WPA2-Enterprise 802.1X EAP-TTLS with PAP
- Device receives cloudlet credentials and validates
- Devices sends its credentials for validation



Communication between the mobile device and the cloudlet is encrypted at the transport and message level

API Requests
- Device exchanges encrypted messages with the cloudlet
- Each exchange is validated against authorized device list

Device Credential Revocation
- Automatic due to timeout: Bootstrapping requires setting up mission duration
- Manual due to known loss or compromise: Cloudlet Manager component has revocation option

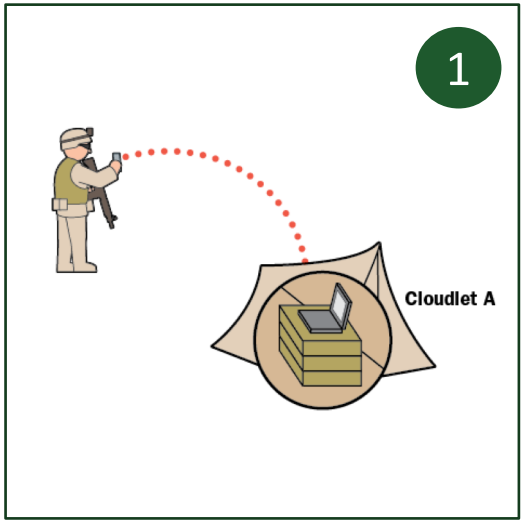
Secure Service VM Migration 1

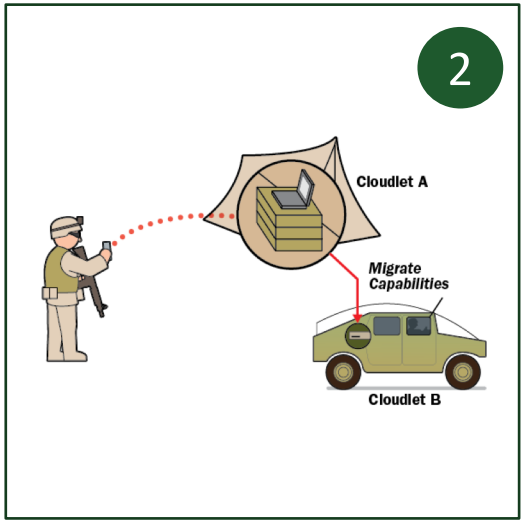
Service VM Migration involves transferring a running service VM on a source cloudlet to a target cloudlet

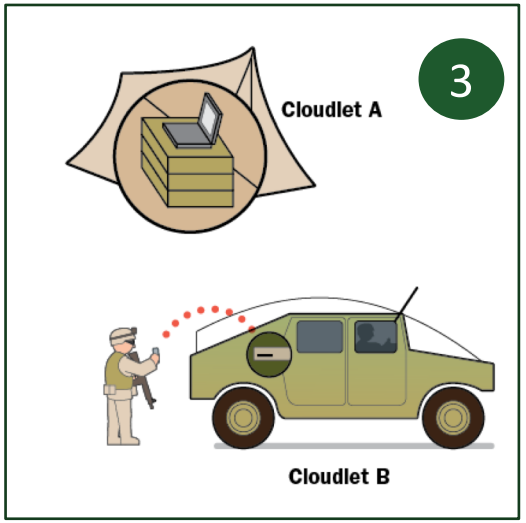
- VM migration
- Device "migration"

Challenges

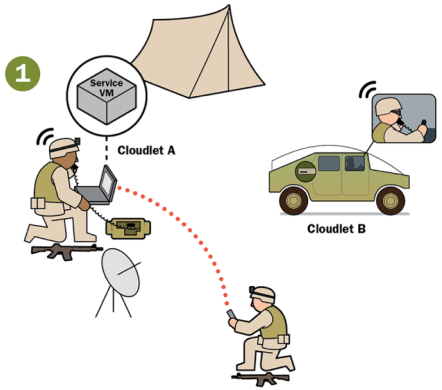
- Establishing trust between cloudlets for credential exchange
- Transferring device trust from source to target cloudlet





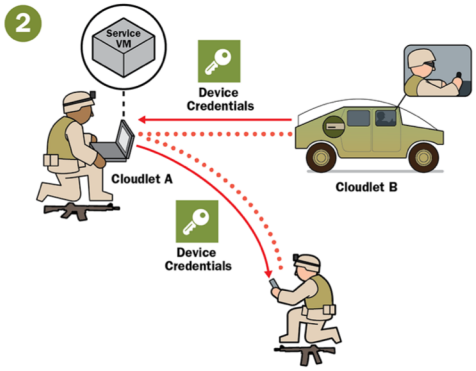


Secure Service VM Migration 2



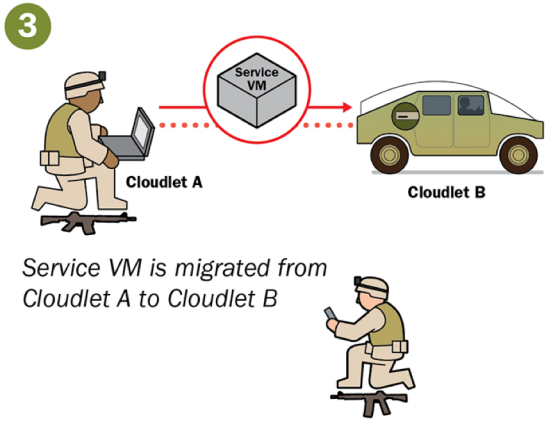
Cloudlet Admins exchange temporary keys using their radios

Cloudlet Pairing
- Cloudlet Admins exchange temporary keys over voice
- Keys are used to setup a temporary channel
- Cloudlet credentials are exchanged over the temporary channel



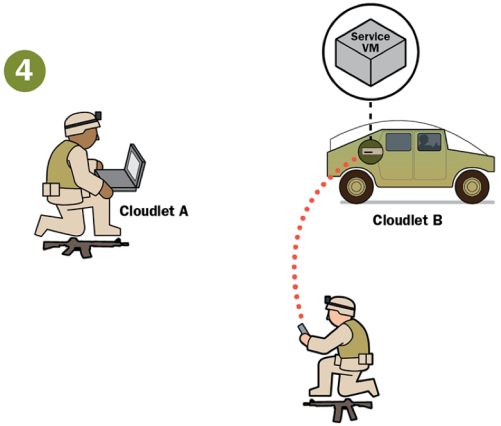
Cloudlet B generates and sends device credentials to Cloudlet A

Device Credential Generation
- Cloudlet A discovers and connects to Cloudlet B using exchanged credentials
- Cloudlet B generates new credentials for Device
- Cloudlet B sends credentials to Device via Cloudlet A



Service VM is migrated from Cloudlet A to Cloudlet B

Service VM Migration
- Cloudlet A migrates Service VM to Cloudlet B



Device connects to the migrated Service VM on Cloudlet B

Device Connection
- Device connects to Cloudlet B using new credentials
- Client App on Device connects to Service VM running on Cloudlet B