Carnegie Mellon University
Software Engineering Institute

Demonstrating Tactical Cloudlet Technology for the U.S. Marine Corps

Reason for Adopting Tactical Cloudlet Technology

Tactical cloudlets are discoverable, forward-deployed compute nodes that can be hosted in the field 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 dismounted warfighters
- collection points for data heading for enterprise repositories

USMC Plans for Tactical Cloudlet Technology

The U.S. Marine Corps (USMC) envisions a phased approach to adopting tactical cloudlet technology at the front edge of the battlespace.

First, USMC commissioned a study by Northrop Grumman to identify tactical computing hardware that could be used as tactical cloudlets. Next, in this work. USMC asked the Carnegie Mellon University Software Engineering Institute (SEI) for a demonstration of its tactical cloudlets software on an identified hardware arrangement to support edge operations.

In future work, USMC expects to instantiate SEI software on a mobile device/tablet interacting with a tactical cloudlet, with a prototype demonstration of a combination of capabilities to support a Tactical Recovery of Aircraft Personnel (TRAP) operation scenario. Following that, USMC plans to deploy tactical cloudlets in the field.

The Reason USMC Worked with the SEI: Tactical Cloudlets Software Expertise

Recognizing the SEI's multiple-year research and development (R&D) of tactical computing and communications and its innovation of software to implement tactical cloudlets, USMC tabbed it to help prototype and demonstrate the technology.

The SEI leveraged its R&D in of tactical computing and communications, edge analytics, and delay-tolerant networking.

In addition to its technology expertise, the SEI also offers prototyping capability to develop and produce an initial small-scale demonstration of porting a cloudlet manager to tactical computing hardware.

SEI's Role: Demonstrate Applicability of Tactical Cloudlets Software

In this work, the SEI

- ported its tactical cloudlet software to tactical computing hardware identified for USMC by Northrop Grumman.

- developed a prototype demonstration of its speech recognition application interacting with the software on the hardware

Importance of this Work

Personnel at the front edge of the battlespace require access to cloud resources to perform their missions. However, tactical environments have disconnected-intermittent-limited (DIL) connectivity, which means that access to computation and data in the cloud is not always possible. The tactical cloudlet enables organizations to “carve out” a piece of the cloud and make it accessible to personnel operating in tactical environments in a secure, reliable, and timely manner on a tactical cloudlet.

Related SEI R&D

KD-Cloudlet Software

In 2017, SEI released version 3.0 of its implementation of tactical cloudlets, KD-Cloudlet. The new version contains code for secure VM migration between tactical cloudlets based on secure key generation and exchange in the field. This enhancement addresses the mobility of cloudlets in the field, as well as in dynamic missions, wherein a mobile user of a cloudlet might need to migrate active capabilities to another trusted cloudlet. It also includes an OSv version of the speech recognition application to demonstrate the use of tactical cloudlets with small-sized VMs. KD-Cloudlet software is freely available on GitHub.

Tactical Computing and Communications

This project worked toward a goal of developing architectures and technologies to provide efficient and secure computing and communications for teams operating in tactical environments, in particular

- Trusted Identities in Disconnected Environments for securing communication between mobile devices and cloudlets operating in tactical environments
- Secure VM Migration for enabling secure migration of capabilities between cloudlets in tactical environments
- Delay-Tolerant Data Sharing for efficient information sharing between nodes in tactical (DIL) environments

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.

DM18-0626