August 2012 System Assessment and Validation for Emergency Responders (SAVER)

Homeland Security
Science and Technology

TechNote

U.S. Department of Homeland Security
SAVER
System Assessment and Validation for Emergency Responders

The U.S. Department of Homeland Security (DHS) established the System Assessment and Validation for Emergency Responders (SAVER) Program to assist emergency responders making procurement decisions.

Located within the Science and Technology Directorate (S&T) of DHS, the SAVER Program conducts objective assessments and validations on commercial equipment and systems and provides those results along with other relevant equipment information to the emergency response community in an operationally useful form. SAVER provides information on equipment that falls within the categories listed in the DHS Authorized Equipment List (AEL).

The SAVER Program is supported by a network of technical agents who perform assessment and validation activities. Further, SAVER focuses primarily on two main questions for the emergency responder community: "What equipment is available?" and "How does it perform?"

For more information on this and other technologies, contact the SAVER Program Support Office.

RKB/SAVER Telephone: 877-336-2752
E-mail: saver@dhs.gov
Website: https://www.rkb.us/saver

This SAVER TechNote was prepared by the Eastern Kentucky University Justice and Safety Center under Cooperative Agreement EMW-2005-CA-0378 with the Federal Emergency Management Agency, DHS.

Reference herein to any specific commercial products, processes, or services by trade name, trademark, manufacturer, or otherwise does not constitute or imply its endorsement, recommendation, or favoring by the United States Government. Neither the United States Government nor any of its employees make any warranty, expressed or implied, including but not limited to the warranties of merchantability and fitness for a particular purpose for any specific commercial product, process, or service referenced herein.

Mobile Computing Through the Cloud

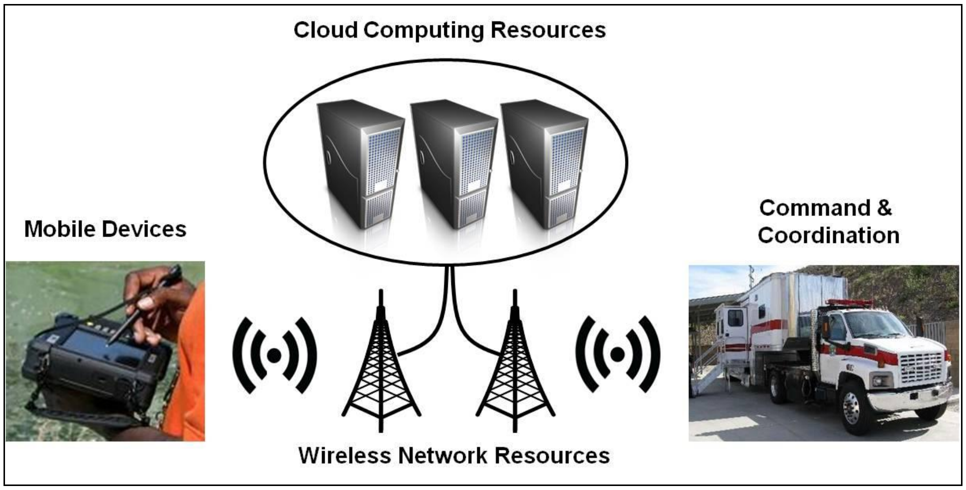
The proliferation of mobile broadband Internet access and new mechanisms to pool computing resources remotely ("cloud computing") has enabled agencies to deploy small devices in the field capable of accessing sophisticated applications and vast amounts of data. It has also offered incident personnel with a common operating picture as situation updates are made real-time and network-wide. This equipment falls under the following AEL categories: 04HW-01-MOBL (mobile computer devices) and 04HW-01-INHW (integrated computer hardware).

Technology Overview

The National Institute of Standards and Technology (NIST) defines cloud computing as "on-demand network access to a shared pool of configurable computing resources" (Mell & Glance, 2011). Cloud computing centralizes the management of large-scale computing capabilities that may consist of hardware (e.g., servers, storage) and software applications (e.g., operating systems, security), providing operational and information technology (IT) management benefits. For example, mobile device requirements are minimal in a cloud computing configuration, often only needing access to a web browser.

Configurations and Models

Until recently, response agencies have operated in the field using a thick client configuration. This configuration confines field users to the computing resources available on the device itself, which may limit flexibility when it comes to managing applications or accessing data. Made available through the expansion of wireless local and wide area networks, thin client configurations are gaining popularity among response agencies. In this type of configuration, the services and applications are "served" to end users over a network rather than stored on responders' mobile devices. Complex



Integration of Cloud Resources

processing applications may be interfaced and used from basic computing hardware such as a smart phone or other mobile computing platform. Cloud computing is comparable to variations of thin client configurations.

While many agencies must seek third party vendors to provide the entire cloud computing infrastructure, many agencies today have acquired their own infrastructure and are capable of serving applications and data themselves. Relying on a third party vendor to only provide the hardware necessary for serving applications is one common cloud computing model. Regardless of hardware ownership, agencies may prefer to deploy response applications via the cloud such as incident decision support software (e.g., geospatial information, resource management). Agencies also have the option of serving and synchronizing back-end operating systems, databases, and middleware across their entire network.

Opportunities

Mobile devices for interfacing with the cloud may be designed for deployability (lightweight and small in size) since computing is handled by external resources. Through a mobile broadband connection, responders in the field could access vast amounts of information in the form of documents, procedures, and maps. Since databases are managed centrally, near real-time updates to maps and status boards provide all users on the network with a common operating picture, including personnel at command centers.

Variations of cloud computing may also make it easier for IT personnel to manage, maintain, and secure applications for the benefit of all agency personnel. Rather than having to manually update potentially hundreds of separate computers, IT personnel may update the operating system and software on one or more central servers for the benefit of all users on the network, a significant savings in personnel time. Agencies without servers and network equipment, or the funds to purchase that equipment, may rely on third-party vendors to host applications at a price they may find affordable.

Risks

While access to mobile broadband networks is expanding, many responders operate in rural or frontier areas where wireless communications coverage remains weak. Access to networks from in-building spaces may also be a challenge as hardened structures tend to diminish cellular signal strengths even at the lower end of the bandwidth range.

Disasters could also result in damaged and degraded infrastructure as well as overloaded networks. The unreliability of access to networks and need for redundancy may require a thick configuration for field users.

Damaged Infrastructure

Agencies may also have security concerns when it comes to reliance on the cloud, especially in procuring services from a third party vendor. Before procuring a cloud computing service from a private sector company, agencies should closely consider the measures in place to isolate and safeguard agency information from public data and other private data that may be handled by the company. The need for cyber security and the sensitivity of data may lead an agency to host applications on their own IT equipment to closely monitor access.

Example Applications

An evaluation of opportunities and risks may lead agencies to consider hybrid configurations that involve one or more applications managed through the cloud, while other applications critical to mission success and life safety are installed on responders' devices.

Urban Search and Rescue

For example, urban search and rescue personnel operating in an area impacted by an earthquake may need area maps pre-installed on ruggedized computers for quick access during the initial phases of the response. After communications have been re-established in the impacted area, these teams may gain access through the cloud to incident decision support software that includes status boards and incident maps monitored by the incident commander. Less mission critical applications, such as an exercise simulation tool that provides notional scenarios, maps, and situation updates to exercise participants, may be entirely provided via the cloud.

References

Mell, P., & Glance, T. (2011). *The NIST Definition of Cloud Computing (Special Publication 800-145).* Gaithersburg, MD: National Institute of Standards and Technology.

Note: For a description of the methodology and additional references for this TechNote, see the *Ruggedized Computers Selection and Procurement Guide*, which is available by request at https://www.rkb.us/saver.