

## Connecting "Things" to the "Cloud"

### Secure IoT Gateway : Cavium Octeon TX™ + MontaVista CGX®

As IoT (Internet of Things) device market grows into billions of connected devices, one of the most critical components of future Internet of Things systems may be the "IoT gateway". An IoT gateway aggregates sensor data, translates between sensor protocols, processes sensor data before sending it onward and more.

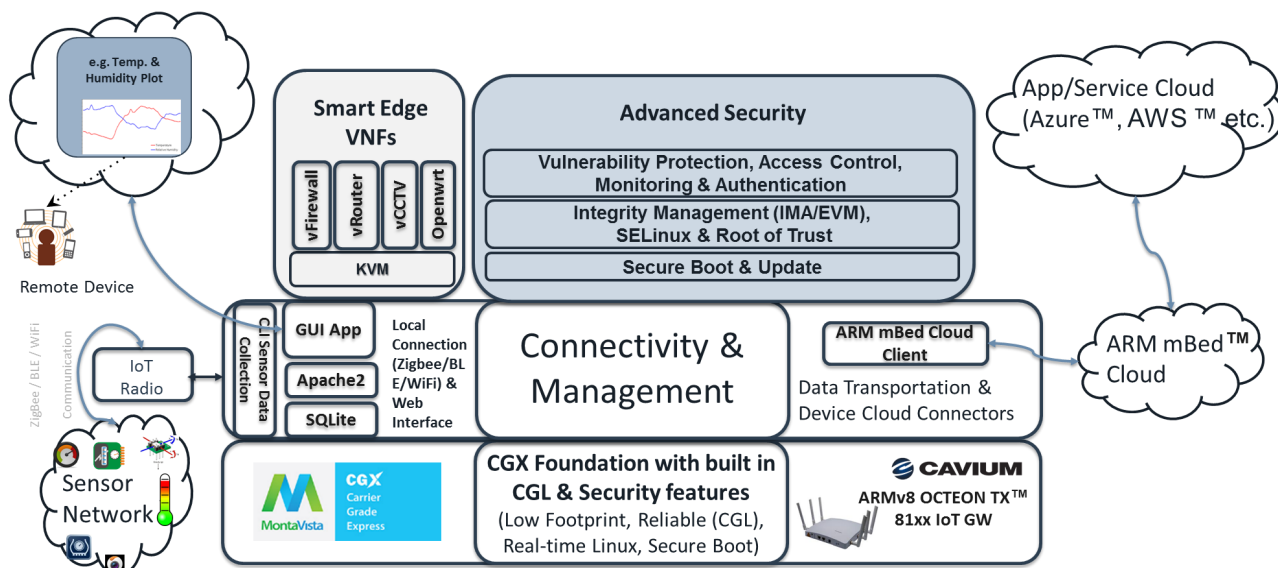


Fig 1: Secure IoT Gateway Prototype with Environment Monitors

MontaVista Carrier Grade eXpress provides necessary software, tools and support to help custom designs, by:

- ◆ **Simple :** Yocto™ based Linux solution with pre-certified Linux BSP (Board Support Packages) on the latest and greatest hardware from our SOC partners. An aptly named, IoT profile along with bring-up support.
- ◆ **Secure:** MontaVista CGX Security profile can be customized to enable secure gateway partitions, utilizing an ARM TrustZone® enabled secure world environment. This offers secure boot, applications including certificate management, secure firmware upgrades, and secure data storage.
- ◆ **Scalable:** As the number of devices proliferates in the enterprise, the gateway will have to handle the increased network traffic and provide device automation, device management, and network access policies. This level of complexity necessitates the selection of a reliable system software like MontaVista CGX® .

#### BENEFITS

- ◆ OUT OF BOX EXPERIENCE WITH PRE-TESTED BSP
- ◆ BUILT IN CONNECTIVITY, RELIABILITY AND SECURITY
- ◆ SECURE KERNEL AND APPLICATION UPDATE
- ◆ Smart Edge with KVM and readymade VNFs
- ◆ PROTOTYPED WITH RANGE OF SENSORS INCLUDING ENVIRONMENTAL MONITORS

#### APPLICATIONS / USE CASES

- CGX Foundation, IoT AND SECURITY PROFILES
- ◆ CONNECTIVITY
  - ◆ RELIABILITY AND
  - ◆ SECURITY PACKAGES
- USE CASES LIKE
- ◆ INDUSTRIAL MONITORING
  - ◆ ENERGY MONITORING
  - ◆ SMART HOME AMONG OTHERS

## Connecting "Things" to the "Cloud"

### Secure IoT Gateway : Cavium Octeon TX™ + MontaVista CGX®

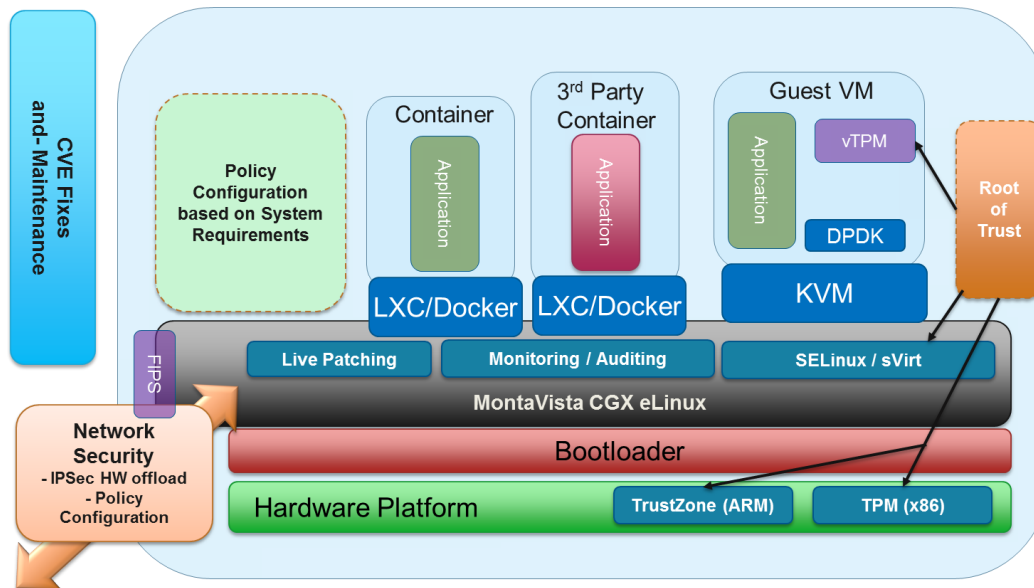


Fig 2: Architectural Design Consideration with MontaVista CGX®

#### SECURITY AND PRIVACY

The issue of safety and security is specially relevant in the case of the internet of things, involving consumer applications which can be potentially hacked. Communications between the things, the gateway, and the cloud service must be cryptographically secured to preserve confidentiality, integrity, and authenticity.

#### End-to-end Encryption

If an attacker were to compromise the IoT gateway, not only the data passing through the gateway is at risk, but control of the physical things connected to it are at risk as well.

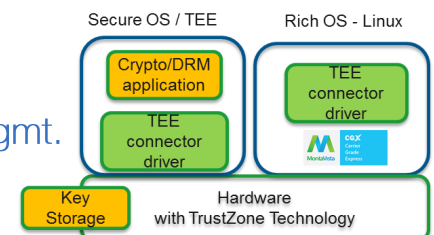
One way to mitigate this problem is to implement true end-to-end, application layer security. Using this strategy, messages are encrypted in a way that allows only the unique recipient of the message to decrypt it, and not anyone in-between. The Allseen Alliance AllJoyn IoT standard has great documentation on how to secure onboarding and cryptographic security in the ecosystem.

#### Integrity Management and Root of Trust

Simply put integrity management in Linux is specifically designed for preventing offline tampering of data. By

combining IMA/EVM and a hardware Root of Trust (like TPM) to provides a chain of attestation through the bootloader, kernel, and user-space, a tamper proof system can be envisioned. These goals are complementary to Mandatory Access Control (MAC) protections provided by LSM modules, such as SELinux and Smack, which, depending on policy, can attempt to protect file integrity.

Fig 3: Integrity Mgmt. & Root of Trust



#### Secure Firmware Updates

Since many IoT devices gateway don't have much in the way of UI or internal storage, an external application and gateway is often required to retrieve and apply firmware updates. To update firmware securely, the system should record current version and new version of the firmware, check for a valid signature on the downloaded firmware upon receipt, and check firmware integrity before firmware installation.

**Secure IoT gateway solution based on CAVIUM OCTEON TX™ is a simple, secure and scalable prototype. It supports a wide array of IoT optimized interfaces engineered to support the secure delivery of IoT services to a wide base of customer use cases.**

***eXpress.Connected.Everything.***

#### About MontaVista Software

MontaVista Software, LLC, a wholly owned subsidiary of Cavium Networks (NASDAQ:CAVM) is a leader in embedded Linux commercialization. For over 15 years, MontaVista has been helping embedded developers get the most out of open source by adding commercial quality, integration, hardware enablement, expert support, and the resources of the MontaVista development community.



All Ways Open

#### MontaVista Software

2315 North First St, 4th FL  
San Jose, CA 95131  
Email: [sales@mvista.com](mailto:sales@mvista.com)  
Tel: +1-408-943-7451