DEVICE SECURITY

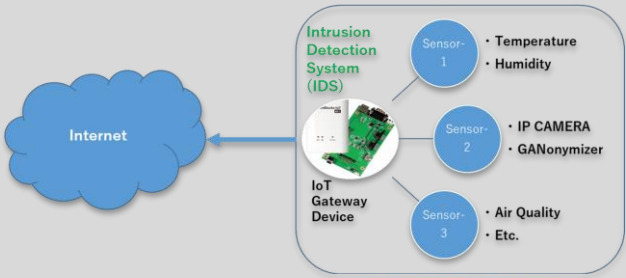
APPLY NOVEL HARDWARE AND SOFTWARE SOLUTIONS TO CREATE SECURE MONITORING IoT DEVICES

Even though current smart city platforms themselves are secured, device level vulnerabilities put the whole system at risk. It is a fact that ensuring device-level security requires tremendous efforts for IoT providers. **M-Sec's Device Security Functional Group** provides a set of methodologies and tools to support development of secure smart city IoT devices on top of the M-sec platform.

FEATURES

- **Secured IoT Device** A hardware based solution to provide an embedded security layer to diverse-purpose IoT devices.

- **Intrusion Detection System (IDS)** A software-based solution to provide a secure IoT mobile sensing platform by monitoring and preventing cyber attacks



KEY BENEFITS

Secure encryption and decryption of data generated by different sensors

Introduction of secure boot mechanisms

Monitoring and reporting, along with the option for blocking malicious traffic matching known signatures

Configured rules to protect IoT devices from a potential attack

SYSTEM REQUIREMENTS

- HW solution apt for STM32-L4 based devices
- HW solution apt for Raspberry Pi-based devices
- SW solution based on Open Source Software (OSS) not needing any licensing.

DID YOU KNOW?

The **Secured IoT Device** hardware and software solution provides IoT devices with mechanisms to assure they are properly protected both at the time of booting and the moment they proceed to send data generated by their sensors, avoiding external interferences and malicious tweaks.

The lightweight **Intrusion Detection System** software has been customized with OS hardening to reduce attack surface, secured communication using Transport Layer Security (TLS), and signature patterns obtained from the testing and analysis in the IoT honeypot, besides other well-known up-to-date attack signature patterns provided by open source resources