

# Making IoT good for business

*Progress in technologies like sensor and networks has been impressive since the term "Internet of Things" was first coined in 1999. Today, mobile Internet is propelling a period of explosive growth in the large-scale commercial adoption of IoT. However, the road isn't completely smooth and industry verticals are slow to jump aboard the IoT train.*

By Jiang Wangcheng





**Cost-effectiveness and convenience**

- Flexible, open architecture and the rapid integration of applications
- A diverse range of access networks
- LiteOS enables the smartification of devices



**Security and reliability**

- Device-side anti-attack capabilities
- Malicious device detection and isolation on the network side
- Cloud platform and data protection
- E2E security standards and policy guidance



**Efficiency and shared success**

- US\$1 billion investment by Huawei to support developers
- OpenLabs opens the capabilities of Huawei's IoT solution
- Huawei jointly innovated and launched a variety of IoT solutions for vertical industries



**A matter of security**

In practice, while IoT services like smart door locks, Internet of Vehicles (IoV) and home security cameras have made life more comfortable and convenient, poor security has opened the floodgates for repeated hacks on IoT equipment. While operators and enterprises have forged ahead with IoT network construction, they cannot deal with the software development required for specific vertical industry scenarios, because the IoT ecosystem and application scenarios are too complex.

For the large-scale commercial use of IoT to take off, the entire industry must come together to build an ecosystem with the following features: cost-effectiveness and convenience, security and reliability, and efficiency and shared success. Huawei extensive forays into the IoT field include tailoring IoT tech

for specific verticals, launching industry solutions, and advancing the commercial use of IoT.

**Cost-effectiveness and convenience**

High service development costs, risks, and complex deployment discourage verticals from investing in IoT. Given this, IoT solution providers should make developing IoT services economical and convenient, with lower barriers to entry.

Huawei's IoT solution comprises chipset and LiteOS for devices, gateways, networks, and a cloud platform. Its IoT cloud services support flexible, open architecture and the rapid integration of industry applications. The full scope of IoT-based service capabilities include device integration, device management, and application enablement. Huawei's vertical

*Huawei offers a diverse range of access networks to meet the demands of IoT access in any scenario.*

application suite provides solutions for Smart Utilities, IoV, Smart Manufacturing and Smart Home.

When enterprises develop applications, they can invoke various open APIs to accelerate the development of industry applications and the launch of new services, including basic northbound APIs (such as secure access, device management, rule engine, and push messaging), industry APIs (including smart utilities, IoV, smart manufacturing, and smart homes), southbound device APIs (such as the sensor ecosystem, gateway ecosystem, and camera and chip module ecosystem). These APIs provide device development enabling suites and serialized agents for device developers.

Huawei offers a diverse range of access networks to meet the demands of IoT access in any scenario. NB-IoT addresses the needs of cellular IoT for low-power, wide coverage, low-cost, and a large number of connections. eLTE (enterprise LTE) uses unlicensed spectrum to support integrated broadband and narrowband services on a single network. This meets enterprises' different production and operations needs and helps them complete digital transformation.

EC-IoT (Edge Computing IoT), that is, enterprise IoT gateways with edge computing power, are widely used in smart elevators and smart buildings. Smart home gateways support home health, entertainment, security, and home automation services, enabling operators to

extend their services from traditional home broadband to smart homes.

With a heavy industry focus on the device side at the moment, Huawei provides the LiteOS IoT operating system, which enables the smartification of devices, quick access to the IoT network, and visualized and simple device management. Huawei LiteOS is a lightweight, open-source IoT operating system that provides unified and open APIs through an open-source model, allowing partners to quickly develop IoT devices for verticals like smart utilities, IoV, smart manufacturing, and smart homes. After a device has been integrated with Huawei LiteOS, it can securely connect to Huawei's cloud platform, which provides complete device management, including visual management on devices, remote firmware and application software upgrades, and device fault location.

## Security and reliability

The outlook has not been optimistic for IoT security so far, with multiple instances of hacks against devices like cameras, smart locks, and even children's watches. In October 2016, the Mirai virus attacked a huge number of smart cameras, smart gateways, smart home appliances and other vulnerable IoT devices, turning them into botnets for hackers. There is also widespread industry concern over security issues surrounding IoV and smart cars; for example, in 2015 Chrysler was forced to recall 1.4 million vehicles due to the vulnerability of its in-vehicle networking equipment.

## Huawei's answer

Huawei proposes a "3+1" deep security defense system with device-side anti-attack capabilities, malicious device detection and isolation, platform and data protection, and secure control and O&M on the network side.

As many IoT devices have limited storage and computing resources, Huawei has designed lightweight IoT secure connection protocols to support distributed authentication and meet low RAM and ROM requirements, solving communication security issues between IoT devices and cloud.

On the network side, Huawei security solutions provide traffic surge prevention. With a deep learning design based on malicious behavior detection, the solution can quickly identify and isolate malicious devices.

In terms of platforms and data protection, Huawei uses cloud platforms and big data security technologies to prevent IoT platform data from being attacked or leaked. Personal data in the cloud is also fully protected, in line with local privacy laws.

Huawei has also built a set of E2E security standards, including daily security assessments, automatic

security awareness, and other security risk alarm and detection capabilities. These are designed to guide O&M personnel in operations and establish security control mechanisms.

Beyond technology and products, Huawei is also contributing to IoT security by working with other ecosystem players.

First, Huawei provides strong support to partners as part of its device security solution. Huawei is a leader in designing device security and security testing guides. Through its Huawei OpenLabs, which are located throughout the world, Huawei plans to make security testing tools available to its industry partners.

Second, Huawei is helping to develop IoT security standards. It has already proposed an optimized DTLS (DTLS+) protocol and lightweight device authentication method. It also sits on government and industry organizations, encouraging them to increase involvement in IoT security policy guidance and laws, and in constructing the industry ecosystem.

## Efficiency and shared success

In 2015, Huawei announced a US\$1 billion investment to support developers. Huawei has

built 14 OpenLabs in various cities, including Shenzhen, Xi'an, Shanghai, Tokyo, and Dusseldorf. These enable partners to use the open capabilities of Huawei's IoT solutions at any time. Huawei has also jointly built eight OpenLabs with operators, including Vodafone. OpenLabs services include joint solution innovation, integration, and verification to accelerate TTM.

In 2017, Huawei and its partners jointly innovated and launched a variety of IoT solutions for vertical industries; for example, smart water services with Shenzhen Telecom and Shenzhen Water, and smart meters with the module manufacturer u-blox and Portugal Telecom to automate electricity data collection, reduce line loss rate, and minimize arrears. Huawei has developed a smart parking solution with Shanghai Unicom and SureKAM that collects parking information and queries, reducing manpower costs, raising the utilization of parking spaces, and increasing parking revenues. Huawei worked with China Telecom to provide a NB-IoT-based smart lock system for the bike sharing giant ofo, slashing bike unlocking speed and greatly improving customer satisfaction.

As a positive contributor to the IoT industry, Huawei believes that integration and partnerships are at the heart of a thriving IoT ecosystem. 