Edge Computing Technologies to Connect the Missing Link of IoT

YOKOTA Haruki, ODA Shinya, KOBAYASHI Tsukasa, ISHII Daiji, ITO Takahiro, ISOZUMI Atsuhiro

Abstract

As a result of the advancement of IoT, the settings of its new applications, for which a real-time capability are required, are increasing. However, because of the response time and communication costs it is sometimes difficult to upload data from sensors and camera images to the cloud environment in order to perform analyses and actuations. A concept that is recently attracting attention as a solution to these issues is edge computing. Based on the concept that edge computing can expand the settings of IoT usage by complementing the cloud, NEC is advancing R&D into technologies suitable for its implementation. Among such technologies introduced in this paper are the autonomous distributed cooperative technology, edge engine acceleration platform and edge SW as well as the relevant IoT security procedures to be located at the edge.

Keywords
edge computing, autonomous distributed cooperative technology, IoT security, edge accelerator, zero-touch configuration

1. Introduction

Under the advancement of IoT, the scenarios of its new applications for which a real-time capability is required are increasing. These include the auto operation of automobiles, UAVs (Unmanned Aerial Vehicles) and robots and the simultaneous authentication of multiple persons in a crowd. However, in such scenarios it is sometimes difficult to upload the data from sensors and camera images to the Internet cloud environment every time and to perform analyses and actuations (execution instructions to equipment) due to the response time and communications costs. From the viewpoint of privacy, the transmission of image data to the cloud environment and saving it there are sometimes issues of concern. A concept that is recently attracting attention as offering a solution to these issues is the new technology of edge computing.

The fog computing* term is also used in a similar manner and the basic idea is common to both terms. In collaboration with enterprises and organizations sharing the same awareness NEC participates in the OpenFog Consortium that advances the standardization of fog computing with the purpose of improving interoperability.

In the rest of this paper, the authors introduce some of the technologies that NEC is developing in consideration of the need for the implementation of edge computing. These include the autonomous distributed cooperative technology, the edge engine acceleration platform and edge SW as well as the IoT security around the edge.

2. Autonomously Distributed Cooperative Technology

With edge computing, a large quantity of data processing operations are generally executed across a large number of edges and clouds. Especially, in the applications settings of smart cities and retail chain stores, the number of edge settings reaches tens of thousands and these are distributed geographically. This situation requires laborious optimized design in support of the effective deployment of applications in the execution environments.

* The "Fog" of fog computing means the possibility of a wide range of combinations in the multilayer network configured by the edge and cloud layers. The edge computing concept adopted by NEC has comprised such a multilayer network since its start.

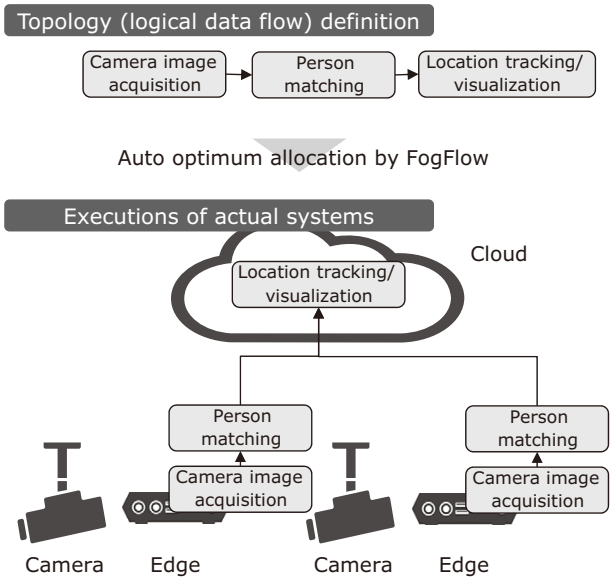

Fig. 1 Operational principles of FogFlow.

FogFlow is the task distribution optimization technology that NEC adopts in performing R&D to deal with the above issue. When the flow of data processing in an IoT system is defined logically as a topology (flow of several tasks for data processing), FogFlow allocates tasks by distributing them optimally among several edges and clouds. This is achieved by considering the geographical relationships between the nodes that actually process data (edges and clouds) and by using the container technology (Docker). The nodes are connected automatically so that they may be executed as an inclusive system (**Fig. 1**).

For example, when it is required to discover a specific person (blacklist or lost child) from the images of several cameras, the person matching the processed data is allocated to the cameras or to the edge to which the cameras belong and the location tracking and visualization processing is allocated to the cloud. This makes it unnecessary to upload the raw camera images with a large data quantity to the cloud, thereby reducing the communication costs and also enabling helpful privacy considerations.

NEC intends to continue to advance the FogFlow technology in aiming at a higher degree of autonomy such as the automatic task reallocation according to the performance characteristics and the load situations of nodes and networks, automatic task recovery in the case of a fault, etc.

3. Edge Engine Acceleration Platform

IoT edge computing handles various data acquired from various sensors. Among these activities, image recognition using images acquired from cameras presents the following issues.

(1) Network infrastructure arrangement and communication costs for collecting huge data of images. The data generated by a single HD camera is as much as 80 GB per day and it is not realistic to send all of such image data to the cloud.

(2) A huge amount of processing is required for such a large quantity of data. As the edge is subject to important restrictions in its installation environments (power, environmental resistance, etc.), such processing is not possible with a power-saving, low-performance CPU that is usable at the edge.

Originating from the mobilization of NEC's HW/SW technologies, the edge engine acceleration platform solves the above issues by means of advanced AI processing on the edge that has previously been regarded as being difficult to achieve. Specifically, it makes the above procedure possible by combined use of the FPGA with high power efficiency and a power-saving CPU and additionally by the optimum implementation of algorithms.

For example, at NEC we have configured the NeoFace face recognition engine as an FPGA. NeoFace is software described in C++, and implementing it in FPGA has allowed us to achieve a 100 times higher performance per watt consumed power (20x performance and 1/5 power consumption) (**Fig. 2**). This has enabled new usage settings, such as the simultaneous recognition of multiple faces using high-definition 4K movie images.

The key to this achievement was how to let the AI processing algorithm implemented as software run optimally on the FPGA, or in other words, how the performance could be improved by conversion from software to the FPGA RTL (Register Transfer Level). Many EDA (Electronic Design Automation) and FPGA vendors are challenging this issue, but their conversion level is still lower than that of skilled FPGA engineers.

On the other hand, NEC possesses a prior technology called the CyberWorkBench that excels in performance improvements by auto parallelization compared to competitors' tools. In the present study, NEC proceeded to the auto conversion of AI processing software by using CyberWorkBench as the edge engine acceleration technology conversion engine.

NEC is also advancing implementation of common platforms for FPGA development so that software engineers can attack FPGA development more easily (**Fig. 3**). An AI engine developed by a software engineer is turned into RTL using an engine such as CyberWorkBench and

we are preparing a framework containing drivers, RAS functions and update functions that may be used as a common platform for it.

For the first usage case of the common platform, we are advancing conversion of a car license plate recognition engine that we have been developing over many years into an FPGA. Use of the same platform as CyberWorkBench has succeeded in significantly reducing the development amount and of reaching the operable level in about half the time usually required.

As a future project, we are aiming at letting the edge equipment operate dynamically by changing the FPGA images of edge devices and CPU software via delivery from the cloud. This will enable implementing operations linked with the cloud and other edge devices as either a part of or the core of the autonomous distributed cooperative operation described in section 2 above. This development is proposed so that the user, engine developer and system designer need not perform special design procedures for the FPGA and that the FPGA auto conversion framework based on CyberWorkBench even enables the auto division of the FPGA images and CPU software. NEC is planning to expand the world of edge computing by offering such attractive contributions.

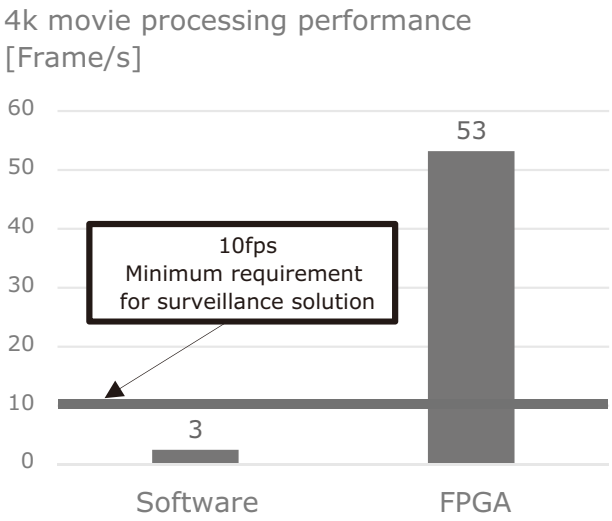

Fig. 2 Comparison of the processing performances of CPU and FPGA.

4. Edge SW

What is important with IoT is to quickly verify feasibility from the technological and business aspects and to promote an improvement cycle. In addition, it is also required to develop and update edge applications quickly. The edge SW improves the portability of applications on edge devices and supports an improvement cycle both in the aspects of development and operation. Its features are as described in the following.

(1) Provision of a common API by abstraction

Connection with sensors, HW of the edge and connection to the Cloud are abstracted to provide a common API that allows the development of applications on the edge without awareness of the HW. The applications developed using the common API can be run on different sensors and edge devices, so that the portability of the applications is increased (**Fig. 4**).

(2) Commercial deployment with zero-touch configuration

When an IoT system involving tens of thousands of edge devices is installed nationwide, it is hard to

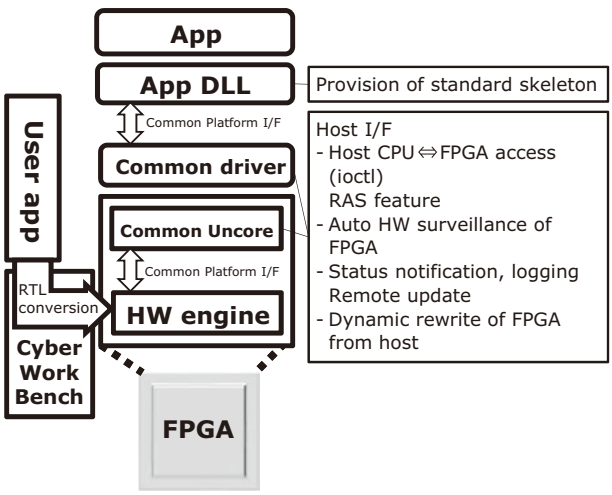

Fig. 3 Common platform for FPGA applications.

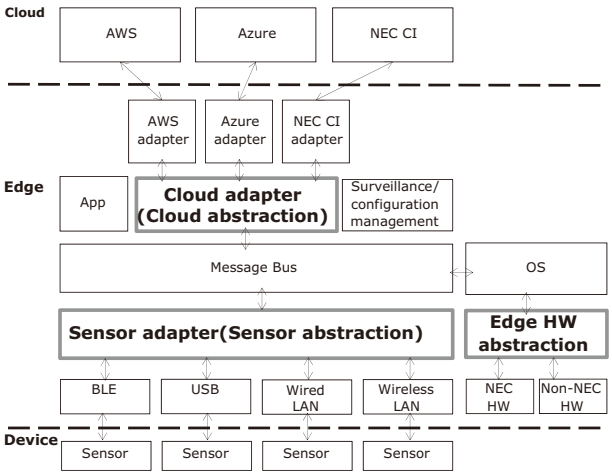

Fig. 4 HW abstraction by edge SW.

assign maintenance personnel to each edge device for its setup. This makes it important to facilitate the edge device setup and enable remote updating as required during operation. The idea of facilitating the edge device setup is called "zero-touch configuration" or "zero-touch provisioning." NEC is developing technologies to enable consistent execution from setup to administration during operation.

To be more precise, a unique ID is assigned to each edge device and the device IDs and setup details are registered in the cloud. This enables auto setup by simply connecting the edge device to the cloud.

Even after the start of operation of the cloud applications information (app names, versions, etc.) of each edge device the applications can be added or updated per edge via control from the cloud so that maintenance costs may be reduced significantly.

As the NEC IoT platforms provide these functions as standard, they enable installation/maintenance expense reduction and quick system installation.

5. IoT Security Issues Surrounding the Edge

5.1 Issues of IoT Security

The major security threats for IoT are illegal accesses and spring boarding that are not new issues. However, there are important secondary issues due to the differences between IoT and conventional ICT.

(1) The SW implementation should be compact and able to operate at a high speed and low load even with a low-priced HW that features few resources.
(2) Security measures should be possible even with devices that use the NW (Network) connection system without security functions.
(3) Autonomous measures should be possible to enforce locally even in an unstable NW connection status.
(4) Maintenance and administration of a large number of devices should be possible remotely without requiring human labor.
(5) Measures should presuppose illegal equipment connections and malfunctions.
(6) Measures should put emphasis on safety and continuous operation.

These issues are particularly important in the connectivity (edges and networks connected to edges) domain.

5.2 NEC's IoT Security Technology for Edge Computing

While the security measures in the connectivity domain are becoming urgent, the available security technologies are limited. At NEC, we are focusing development on the technologies for the connectivity domain, which is one of the weaker points in the entire IoT security area. Below we introduce the Device Security technology, which is one of the IoT security technologies for edge computing that features application of communication virtualization by means of SDN (Software-Defined Networking) to the device communication security.

The Device Security technology is an application of NEC's proven OpenFlow technology to edge computing in order to implement a distributed SDN that does not need an external SDN controller. It also expands the mechanism of OpenFlow presupposing a wired LAN for a wireless interface. Even when a malicious third party penetrates the device, the communication restriction by the virtual NW layer of the SDN preempts a threat such as an information leakage, etc. to the communication (**Fig. 5**).

Technologically speaking, it is an application of the operating principles of OpenFlow to the communications security mechanism of whitelist type edge computing and therefore it has the following features.

- Communications whitelist that can easily be set by the user via abstraction.
- Real-time detection of abnormal communications not foreseen by the system

The IoT system uses a huge amount of devices in the field and the network setup and configuration variations increase as a consequence. For example, in order to set communications whitelists such as a filtering provided as standard with the Linux OS, it generally necessitate a thorough consideration for the NW setting, so the setting gets complicated when variations increase. In addition, since the IP addresses of destinations and sources are assigned by the DNS or DHCP, they are difficult to be identified by people, so the bar to be crossed for securi-

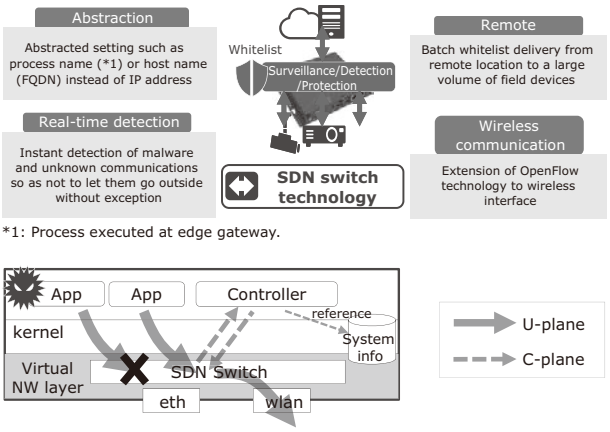

Fig. 5 Features and configuration of Device Security.

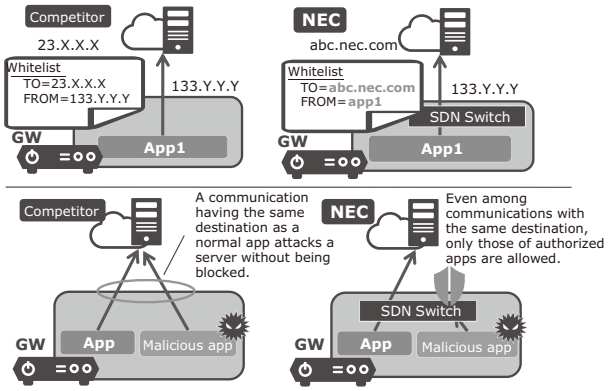

Fig. 6 Abstracted whitelist.

ty management tends to become higher.

The Device Security technology converts (abstracts) the packet ID information such as the IP addresses or port numbers into names easily recognizable by humans, such as the process names or host names (FQDN: Fully Qualified Domain Name), and compiles them in a specifiable communications whitelist.

The whitelist of process names can facilitate the setting and enable restriction of transmission destinations per process, so that even when there are several communications with the same destination, the possibility of restricting only the unforeseen ones is featured (**Fig. 6**).

Using the mechanism of OpenFlow that "inquires of the controller about handling of unknown flow detected" by the SDN switch, it is possible to detect communications generated from processes not registered in the whitelist, together with the process names in real time. This function is expected to be applicable to the detection of the IoT malware that has recently been proliferating.

The communication control of the Device Security technology is performed autonomously by devices that include gateways. This means that a secure, scalable IoT system can be built based on the autonomous distributed control that is characterized by the whitelist-based simultaneously centralized delivery of policies from the cloud and the autonomous flow-related control by the devices.

Part of the present technology has been adopted at the edge gateways provided by NEC for the IoT.

6. Conclusion

In the above, we introduced some of the technologies being developed by NEC that support edge computing. We are currently developing a wide variety of edge computing technologies based on the idea that the use of edge computing will expand the settings of IoT use and enable solutions of social issues. We would like to advise you that we will be delighted to accept inquiries from those who are interested in this topic.

Authors' Profiles

YOKOTA Haruki
Senior Manager
IoT Platform Development Division

ODA Shinya
Senior Manager
IoT Platform Development Division

KOBAYASHI Tsukasa
Manager
IoT Platform Development Division

ISHII Daiji
Manager
IoT Platform Development Division

ITO Takahiro
Manager
IoT Platform Development Division

ISOZUMI Atsuhiro
Manager
IoT Platform Development Division

The details about this paper can be seen at the following.

Related URL:

CyberWorkBench
http://www.nec.com/en/global/prod/cwb/index.html

OpenFog Consortium
https://www.openfogconsortium.org/

Edge gateway (in Japanese)
http://jpn.nec.com/iot/platform/egw/

Information about the NEC Technical Journal

Thank you for reading the paper.
If you are interested in the NEC Technical Journal, you can also read other papers on our website.

Link to NEC Technical Journal website

Japanese English

Vol.12 No.1 IoT That Supports Digital Businesses

Vol.12 No.1
October 2017

Special Issue TOP

Remarks for Special Issue on IoT That Supports Digital Businesses
NEC's IoT Operations That Support Digital Businesses

Papers for Special Issue

Platforms built to support IoT
An IoT Platform to Support Business Transformation - "NEC the WISE IoT Platform"
Edge Computing Supporting Customer Values in the IoT Era
Edge Computing Technologies to Connect the Missing Link of IoT
Case Studies of Edge Computing Solutions

IoT solutions that offer value to customers
NEC Industrial IoT - For Manufacturing in the Age of IoT
Warehouse Product Inspection System Achieves Work Efficiency and Quality Improvements
Warehouse Staffing Optimization Solution Using Autonomous and Adaptive Control - NEC's latest AI technology
Human-Oriented IoT Solutions Using Hearable Technology from NEC
Video Streaming Technology That Supports Public Safety
IoT and AI Innovations for the Retail Industry
Wireless Networking Technology for Real-time Remote Control of Factory Equipment: Wireless ExpEther
Lightweight Cryptography Applicable to Various IoT Devices
PoC of AI Demand Forecast Deployment in the NEC Group's Manufacturing Facilities from an Ethnographical Perspective

General Paper

"My Number" Collection Service Utilizes Several Key Image Recognition Technologies