# Security Requirements and Technologies for Smart City IoT

SASAKI Takayuki, MORITA Yusuke, KOBAYASHI Toshiki

## Abstract

While the Smart City enables efficient City management, it involves the risk that the system may be targeted by cyberattacks. This paper deals with the security requirements necessary for secure smart city management and the security functions needed to meet them. In addition, considering the features of Smart City IoT that handles a variety of data and installs devices throughout the streets, this paper also explains that the security requirements specific to the Smart City IoT should satisfy a flexible information distribution control and support the protection of the IoT devices. Furthermore, this paper discusses technologies for meeting such requirements (Secure data distribution platforms and anti-tamper mechanisms of the IoT devices).

Keywords
Smart city, IoT, security

## 1. Introduction

The Smart City is one that can be managed efficiently by the active use of the IoT (Internet of Things) and its use cases cover a wide range, from disaster prevention to tourism and environmental protection. On the other hand, as the introduction of IoT has connected City management systems to networks, the risk that the systems may become a target of cyberattacks has been a consequence. It is reported that a vulnerable traffic system that is susceptible to being hacked already exists. Such an attack on a smart city system may lead to the paralysis of vital urban functions. Moreover, since the smart city handles closed data such as personal information as well as open data, the optimum management of such data becomes necessary.

This paper discusses the security requirements that the IoT system supporting the Smart City (hereinafter the "Smart City IoT") should meet by focusing on the requirements proper to the Smart City IoT. Other security requirements are common to those of IT systems and include authentication/permission, inhibition of unnecessary communications and security operation/administration (IoT device management, vulnerability/patch management, and incident response, etc.) These general security requirements are brought together in the Cloud Control Matrix[1].

## 2. Security Requirements Proper to the Smart City IoT

For the security requirements proper to the Smart City IoT, NEC has developed a smart city function model based on the documents issued by International Electrotechnical Commission[2] and European Union Agency for Network Information Society[3]. The threats have been sorted out using a threat analysis technique called STRIDE. Based on the results, the authors will show the security requirements proper to the Smart City IoT below in this paper. Specifically, the authors will clarify the security requirements based on features of the Smart City IoT that handles various data and the installation of devices throughout its streets.

**(1) Prevention of data leaks and falsifications**

As one of the Smart City IoT's features, both the open and closed data is handled together. For example, touristic information is basically open data

and the personal part of healthcare data is closed data. In addition, as for highly precise traffic congestion information linking an event information system or a traffic control system, information is expected to be exchanged between the various systems. In consequence, it is required to prevent leaks and the falsification of information, even in environments where a variety of data types and diverse inter-service linkages exist together.

**(2) Prevention and discovery of device tampering**
For ordinary IT systems and smart factories, the IoT devices are installed only at the premises. In the case of the Smart City IoT, the devices are installed throughout the city streets, so that they are easy to access for the attackers. Therefore, considering the risk of an attacker accessing a device directory and carrying out data falsification or device tampering, it is essential to quickly discover tampered or illegal devices. In addition, robustness is required for the entire system from IoT devices to the cloud. This is because a Smart City IoT is composed of IoT, gateways, servers, computers and so on, and that the attacker aims at the weakest part of the system, which makes it necessary to fine tune all of the devices in order to improve the robustness of the entire system.

## 3. Security Functions Required for the Smart City

This chapter describes the functions for meeting the security requirements proper to the smart city, as discussed in chapter 2. It specifically deals with a secure data distribution platform capable of preventing data leaks and falsifications and the tamper detection technology for discovering tampered devices. The presence of both of these technologies ensures the control of information distribution on a reliable platform, thereby serving to implement a secure smart city (**Fig. 1**).

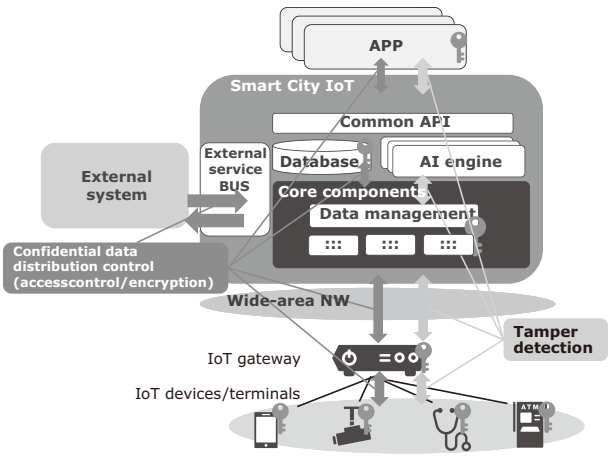


Fig. 1 Security functions required for the smart city.

### 3.1 Secure Data Distribution Platform Preventing Data Leaks/Falsifications

The FIWARE is a Smart City IoT platform developed in Europe. Consisting of a group of components called the GEs (Generic Enablers), it can build platforms for the smart city by combining GEs for information collection and analyses, etc. GEs for security are also available, including Wilma that monitors and controls access, AuthZForce that makes access acceptance decisions based on security policy, and Keyrock that performs user authentications. However, what is available is only the framework of an access control mechanism employing the GEs. In order to control information distribution availability using GEs, it is necessary to examine access control models by actually using the GEs. Describing the security policy using a language called the XACML and preparation of a database for storing the data for use in access control are also required. This constraint has prevented the ease of use of the FIWARE.

To solve this issue, NEC has developed a secure data distribution platform that covers the actual use cases of smart city information distribution and one that is easy to use. The secure data distribution platform controls the distribution of information by assigning attributes to the users. Data and access are controlled based on the relationships of such attributes. Specifically, we analyzed the use cases of smart city and clarified the attributes required for controlling smart city information distribution. Examples of the attributes are departments such as disaster prevention and tourism, and the positions (security levels) of users. Simply assigning these attributes to each user and item of data makes it possible to control the information distribution easily. The distribution ranges may be controlled flexibly by, for example, disclosing confidential data only to those trusted users in specified positions (control according to security level status: gray lines), sharing closed information only inside City Hall (control according to the appropriate department attribute: dotted lines) and opening up information also to the citizenry (black lines) as shown in **Fig. 2**.

### 3.2 Security of communications: Lightweight authenticated encryptions

In addition to the information distribution controls described above, the prevention of data falsification

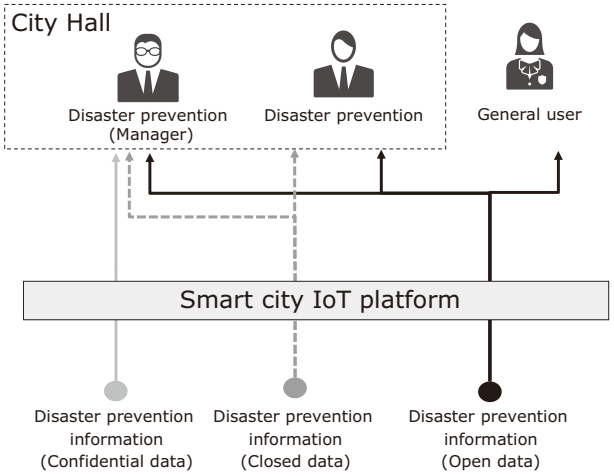


Fig. 2 Example of information distribution in a smart city.

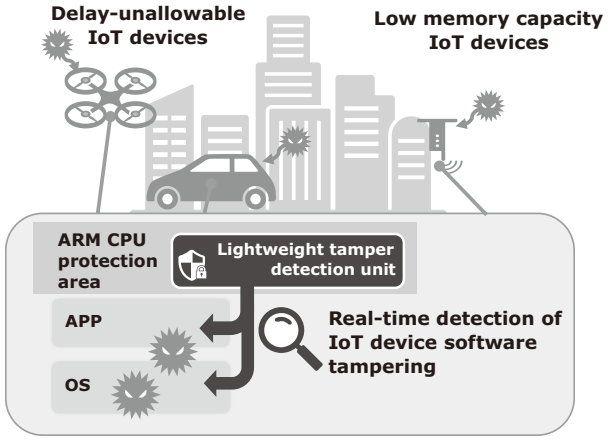


Fig. 3 Lightweight tamper detection technology.

requires data protection even for data collection from devices. Encryption of communications is effective for this purpose but, since IoT devices are restricted in their CPU power and memory capacities compared to computers, it is sometimes impossible to embed the encryption facility in an IoT device. To solve this issue, NEC has developed TWINE[4], a lightweight encryption technology capable of protecting the communications of IoT devices with low memory capacity by means of encryption. When the OTR (Offset Two-Round) authenticated encryption is used additionally, it is possible to implement encryption and falsification detection simultaneously.

### 3.3 Tamper detection technology for preventing/discovering device Tampering

As described in chapter 2, the security of IoT devices at terminals is important for more firmly protecting IoT devices against cyberattacks. However, as also mentioned in section 3.2, some IoT devices cannot introduce security measures due to their CPU power and/or memory capacities. NEC has solved this issue by developing a lightweight tamper detection technology that is applicable to IoT devices with inadequate CPU performances and memory capacities[5](**Fig. 3**). This technology employs TrustZone, the memory function of ARM Cortex-M, in the lightweight (4 KB) installation of a function for detecting tampering of execution codes. It monitors the control instructions sent to a device and examines only the execution code of the function corresponding to an instruction in real time in order to minimize its effect on the IoT device. This function is also applicable to IoT devices for which delays are not permissible. It achieves lightweight installation by focusing on the detection function, so it is incapable of tampering prevention, but a quick response such as via device isolation or recovery is possible after the detection.

## 4. Security in Intercity Cooperation

More than one city may be linked to provide better services. For example, in the case of a disaster, quick delivery of rescue supplies to the stricken areas is made possible by linking the Smart City IoT of multiple cities. When the Smart City IoT systems of several cities are linked for information exchange, they should meet the following security requirements in addition to the Smart City IoT requirements described in chapter 2.

**(1) Federated Authentication**

Federation of user authentications becomes necessary in order to allow users in a certain city to benefit from services provided by another city, or to refer to its data.

**(2) Protection of information handed by other systems**

In addition to the information generated by the platform of a city it is also necessary to manage the information generated in another city and transferred via the linkage services.

**(3) Incident responses across systems**

When the platforms of several cities are linked for operation, it is necessary to perform incident responses across several platforms. This makes it necessary to prepare suitable mechanisms for efficient operations.

Moreover, further to the requirements mentioned above, "(1) federated authentication" can use a standard protocol such as the SAML or OpenID Connect, but "(2) protection of information handed by other systems"

and "(3) incident responses across systems" do not have standardized technologies or protocols. NEC is planning to further advance technological developments as it is expected that such technologies will be needed to support the advancement of smart cities in the future.

## 5. Conclusion

Response to cyberattacks is critical for the stable management of smart cities. In the above, the authors have explained the security requirements of the Smart City IoT and have also introduced security technologies to meet these requirements. In order to create safe and secure societies for the future, the authors are aiming to advance developments and to facilitate the installation of technologies for ensuring the security of Smart City IoT.



## Reference

1) Cloud Controls Matrix Working Group
https://cloudsecurityalliance.org/group/cloud-controls-matrix/#_overview
2) International Electrotechnical Commission
http://www.iec.ch/
3) European Union Agency for Network and Information Security
https://www.enisa.europa.eu/
4) OKAMURA Toshihiko: Lightweight Cryptography Applicable to Various IoT Devices, NEC Technical Journal, Vol. 12, No.1,pp.67-71, October 2017
https://www.nec.com/en/global/techrep/journal/g17/n01/170114.html
5) NEC Press Release: NEC develops tamper detection technology to protect IoT devices, April 2018
https://www.nec.com/en/press/201804/global_20180402_01.html

## Authors' Profiles

**SASAKI Takayuki**
Principal Researcher
Security Research Laboratories

**MORITA Yusuke**
Security Research Laboratories

**KOBAYASHI Toshiki**
Security Research Laboratories

# 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.13 No.1 Sustainable Data-driven City Management


Vol.13 No.1
November 2018

Special Issue TOP

Remarks for Special Issue on Sustainable Data-driven City Management
Start-up of Data Utilization-type Smart Cities

### Papers for Special Issue

**Vision for Data-driven City Management**
Global Perspective for Data-Leveraged Smart City Initiatives
A Paradigm Shift in City Management Practices Targets the Sustainable Society

**Demonstration and Implementation Examples of Data-driven Smart Cities**
Case Study of Data-driven City Management in Cities Abroad
Building a Common Smart City Platform Utilizing FIWARE (Case Study of Takamatsu City)
Initiatives to revitalize regional economies by advancing "*OMOTENASHI*"
— Hospitality offered to foreign visitors to Japan
Case Studies of Data Utilization by Municipal Governments:
Applying Data in Various Fields Such as Financial Affairs, Childcare, and Community Revitalization

**City Management Technologies**
FIWARE, Information Platform for Implementing Data Utilization Based City Management
FogFlow: Orchestrating IoT Services over Cloud and Edges
Security Requirements and Technologies for Smart City IoT
European Trends in Standardization for Smart Cities and Society 5.0
City Evaluation Index Standards and their Use Cases

**Co-creation with Local Communities**
An Introduction to "Partnership for Smart City Takamatsu" as a Platform to Engage in Local Co-creation Activities
Launch of Setouchi DMO — A Co-Creation Venture That Goes beyond the Conventional ICT Framework
Community Co-creation Based on a Comprehensive Cooperation Agreement
A Common-Sense Approach to the Future — Study Group for Co-creation of New Municipal Services

### General Papers

Spin-Current Thermoelectric Conversion — Informatics-Based Materials Development and Scope of Applications
Reducing the Power Consumption and Increasing the Performance of IoT Devices by Using NanoBridge-FPGA
Development of Nano-carbon Materials for IoT Device Applications
Proof of Concept of Blockchain Technology in the Field of Finance Using Hyperledger Fabric 1.0

### NEC Information

**NEWS**
2017 C&C Prize Ceremony