Operations and Management Area Working Group
Internet-Draft
Intended status: Informational
Expires: 17 August 2025

J. Jeong, Ed.
P. Lingga
Sungkyunkwan University
J. Park
ETRI
D. Lopez
Telefonica I+D
S. Hares
Huawei

13 February 2025

An I2NSF Framework for Security Management Automation in Cloud-Based Security Systems
draft-jeong-opsawg-security-management-automation-01

Abstract

This document describes a Framework for Interface to Network Security Functions (I2NSF) in [RFC8329] for Security Management Automation (SMA) in Cloud-Based Security Systems. This security management automation facilitates Closed-Loop Security Control, Security Policy Translation, and Security Audit. To support these three features in SMA, this document specifies an extended architecture of the I2NSF framework with new system components and new interfaces. Thus, the SMA in this document can facilitate Intent-Based Security Management with Intent-Based Networking (IBN) in [RFC9315].

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 17 August 2025.

Copyright Notice

Copyright (c) 2025 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction 2
2. Terminology 4
3. An I2NSF Framework for Security Management Automation 5
3.1. Components with I2NSF Framework for Security Management Automation 5
3.2. Interfaces with SMA-Based I2NSF Framework 6
4. Security Audit System 7
5. IANA Considerations 9
6. Security Considerations 9
7. References 9
7.1. Normative References 9
7.2. Informative References 10
Acknowledgments 12
Contributors 12
Authors' Addresses 12

1. Introduction

Interface to Network Security Functions (I2NSF) defines a framework and interfaces for interacting with Network Security Functions (NSFs) [RFC8192][RFC8329]. Note that an NSF is defined as software that provides a set of security-related services, such as (i) detecting unwanted activity, (ii) blocking or mitigating the effect of such unwanted activity in order to fulfill service requirements, and (iii) supporting communication stream integrity and confidentiality [RFC8329]. The NSF can be implemented as a Virtual Network Function (VNF) in a Network Functions Virtualization (NFV) environment [ETSI-NFV][I-D.ietf-i2nsf-applicability].

This document describes Security Management Automation (SMA) of cloud-based security services in the I2NSF framework. The security management automation includes closed-loop security control, security

policy translation, and security audit. This document specifies an augmented architecture of the I2NSF framework for the SMA services with new system components and new interfaces.

For reliable management for networked security services, this document proposes a network management and verification facility using a secuirty audit system (e.g., remote attestation and blockchain [Bitcoin]). This security audit system can facilitate the non-repudiation of configuration commands and monitoring data generated in the I2NSF framework.

Therefore, the Security Management Automation (SMA) in this document can facilitate Intent-Based Security Management with Intent-Based Networking (IBN) in [RFC9315] for autonomous security services. This SMA is based on Intent-Based Closed-Loop Security Control (ICSC) [ICSC] along with a Security Policy Translator [SPT].

Note that the scope of this document is to propose an extension of the standard I2NSF framework in [RFC8329] such that it can perform security management automation based on Intent-Based Networking (IBN) in [RFC9315]. This document augments the existing I2NSF framework by adding the new features of Security Policy Translator, Closed-Loop Security Control, and Security Audit System to it. For this system augmentation, a system component called I2NSF Analyzer and a new external interface called Analytics Interface are introduced for Closed-Loop Security Control on the basis of the analysis of NSF monitoring data. This monitoring data is delivered from each NSF to I2NSF Analyzer via Monitoring Interface [I-D.ietf-i2nsf-nsf-monitoring-data-model]. I2NSF Analyzer performs the analysis of the NSF monitoring data, and sends the analysis results (e.g., policy reconfiguration and feedback message) to Security Controller via Analytics Interface. For more details, Refer to Section 3 in this document.

Also, note that Cloud or Edge-based Security Service Providers can get benefits by automating security service management in terms of automatic security policy enforcement and feedback-based security policy updates. Eventually, they can save Operational Expenditure (OPEX) significantly by this Intent-Based Security Management with the concept of Intent-Based Networking (IBN) in [RFC9315].

Therefore, the I2NSF Framework can construct Closed-Loop Security Control with a control loop among Security Controller, NSFs, and I2NSF Analyzer in order to adjust the security policy system. This loop uses NSF monitoring data, data analytics, feedback, and policy reconfiguration. The security policy enforcement of a user’s perspective can be done by a Security Policy Translator (SPT) [SPT]. It translates a high-level security policy into the corresponding

low-level security policy for the security policy enforcement. Along with this SPT, Intent-Based Closed-Loop Secutity Control (ICSC) [ICSC], which supports Closed-Loop Security Control according to a user's intent, can be designed and implemented in the I2NSF Framework. Thus, this document specifies the extension of the I2NSF Framework for Security Management Automation based on this ICSC.

2. Terminology

This document uses the terminology described in [RFC8329], [I-D.ietf-i2nsf-applicability], and [SPT]. In addition, the following terms are defined below:

* Security Management Automation (SMA): It means that a high-level security policy from a user (or administrator) is well-enforced in a target I2NSF system. The high-level security policy can be translated into the corresponding low-level security policy by a security policy translator and dispatched to appropriate NSFs. Through the monitoring of the NSFs, the activity and performace of the NSFs is monitored and analyzed. If needed, the security rules of the low-level security policy are augmented or new security rules are generated and configured to appropriate NSFs. This procedure is called Closed-Loop Security Control [ICSC]. This Intent-Based Closed-Loop Security Control (ICSC) is an Intelligent Security Management Automation (SMA).

* Security Policy Translation: It means that a high-level security from an I2NSF User (e.g., administrator) policy is translated to a low-level security policy that can be understood and configured by an NSF for a specific security service, such as firewall, web filter, deep packet inspection, DDoS-attack mitigation, and anti-virus. A Security Policy Translator (SPT) performs this security policy translation for the sake for the I2NSF User [SPT]. This SPT is an subcomponent of Security Controller which is a main component to govern the I2NSF Framework.

* Feedback-Based Security Management (FSM): It means that a security service is evolved by updating a security policy (having security rules) and adding new security rules for detected security attacks by processing and analzing the monitoring data of NSFs.

3. An I2NSF Framework for Security Management Automation

This section describes an extended I2NSF framework for security management automation, where the I2NSF framework is defined in in [RFC8329]. As shown in Figure 1, an I2NSF User can use security functions by delivering high-level security policies, which specify security requirements that the I2NSF user wants to enforce, to the Security Controller via the Consumer-Facing Interface (CFI) [I-D.ietf-i2nsf-consumer-facing-interface-dm].

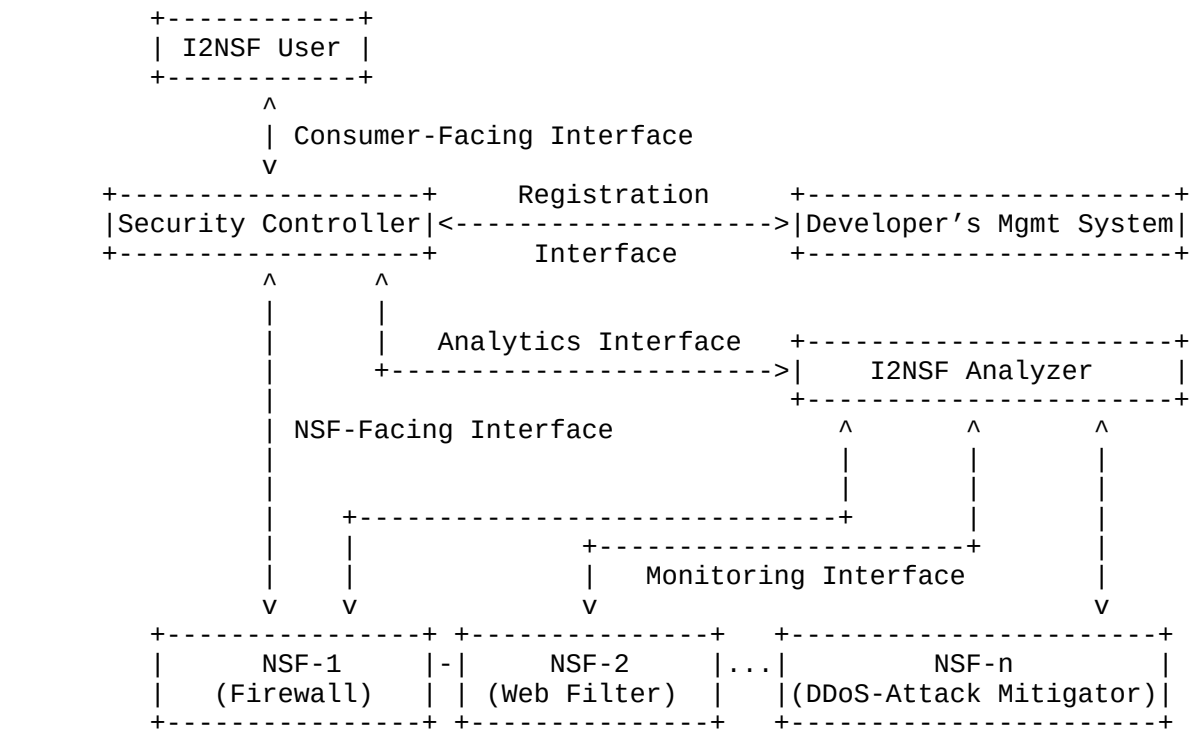

Figure 1: An Extended I2NSF Framework for Security Management Automation

3.1. Components with I2NSF Framework for Security Management Automation

The following are the system components for the SMA-based I2NSF framework.

* I2NSF User: An entity that delivers a high-level security policy to Security Controller.

* Security Controller: An entity that controls and manages other system components in the I2NSF framework. It translates a high-level security policy into the corresponding low-level security policy and selects appropriate NSFs to execute the security rules of the low-level security policy. A Security Policy Translator (SPT) can perform this security policy translation from a high-level security policy into a low-level security policy [SPT].

* Developer’s Management System (DMS): An entity that provides an image of of a virtualized NSF for a security service to the I2NSF framework, and registers the capability and access information of an NSF with Security Controller.

* Network Security Function (NSF): An entity that is a Virtual Network Function (VNF) or Container Network Function (CNF), which is called Cloud-native Network Function, for a specific network security service such as firewall, web filter, deep packet inspection, DDoS-attack mitigation, and anti-virus.

* I2NSF Analyzer: An entity that collects monitoring data from NSFs and analyzes such data for checking the activity and performance of the NSFs using machine learning techniques (e.g., Deep Learning [Deep-Learning]). If there is a suspicious attack activity for the target network or NSF, I2NSF Analyzer delivers a report of the augmentation or generation of security rules to Security Controller.

For SMA-based security services with Feedback-Based Security Management (FSM), I2NSF Analyzer is required as a new I2NSF component for the legacy I2NSF framework [RFC8329] to collect monitoring data from NSFs and analyzing the monitoring data. The actual implementation of the analysis of monitoring data is out of the scope of this document.

3.2. Interfaces with SMA-Based I2NSF Framework

The following are the interfaces for the SMA-based I2NSF framework. Note that the interfaces are modeled with YANG [RFC6020] and security policies are delivered through either RESTCONF [RFC8040] or NETCONF [RFC6241].

* Consumer-Facing Interface: An interface between I2NSF User and Security Controller for the delivery of a high-level security policy [I-D.ietf-i2nsf-consumer-facing-interface-dm].

* NSF-Facing Interface: An interface between Security Controller and an NSF for the delivery of a low-level security policy [I-D.ietf-i2nsf-nsf-facing-interface-dm].

* Registration Interface: An interface between a DMS and Security Controller for the registration of an NSF's capability and access information with the Security Controller or the query of an NSF for a required low-level security policy [I-D.ietf-i2nsf-registration-interface-dm].

* Monitoring Interface: An interface between an NSF and I2NSF Analyzer for collecting monitoring data from an NSF to check the activity and performance of an NSF for a possible malicious traffic [I-D.ietf-i2nsf-nsf-monitoring-data-model].

* Analytics Interface: An interface between I2NSF Analyzer and Security Controller for the delivery of an analytics report of the augmentation or generation of security rules to Security Controller. This interface lets Security Controller get the report for security rules to its security policy management.

For SMA-based security services with FSM, Analytics Interface is required as a new I2NSF interface for the legacy I2NSF framework [RFC8329] to deliver an analytics report of the augmentation or generation of security rules to Security Controller through the analysis of the monitoring data from NSFs.

4. Security Audit System

The I2NSF framework is weak to both an insider attack and a supply chain attack since it trusts in NSFs provided by Developer's Management System (DMS) and assumes that NSFs work for their security services appropriately [I-D.ietf-i2nsf-applicability].

To detect the malicious activity of either an insider attack by a malicious DMS or a supply chain attack by a compromised DMS, a security audit system is required by the I2NSF framework. This security audit system can facilitate the non-repudiation of configuration commands and monitoring data generated in the I2NSF framework.

A security audit system has the following four main objectives:

* To check the existence of a security policy, a management system, and its procedures;

* To identify and understand the existing vulnerabilities and risks of either an insider attack or a supply chain attack;

* To review existing security controls on operational and administrative issues;

* To provide recommendations and corrective actions to Security Controller for further security improvement.

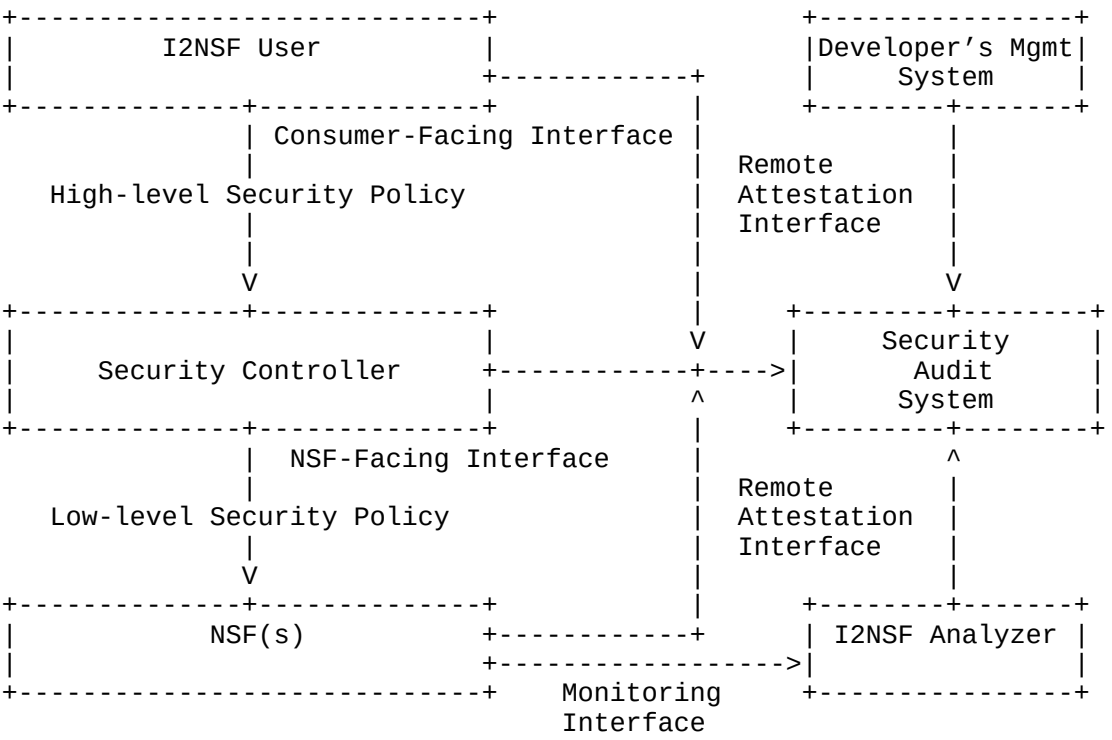

Figure 2: Activity Auditing with Security Audit System

Figure 2 shows activity auditing with a security audit system in the I2NSF framework. All the components in the I2NSF framwork report its activities (such as configuration commands and monitoring data) to Security Audit System as transactions through Remote Attestation Interface [I-D.yang-i2nsf-remote-attestation-interface-dm]. The security audit system can analyze the reported activities from the I2NSF components to detect malicious activities such as an insider attack and a supply chain attack. Note that such a security audit system can be implemented by remote attestation [RFC9334][I-D.yang-i2nsf-remote-attestation-interface-dm] or Blockchain [Bitcoin]. The details of the implementation of the security audit system are out of the scope of this document.

In order to determine a minimum set of controls required to reduce the risks from either an insider attack or a supply chain attack, the security audit system should analyze the activities of all the components in the I2NSF framework periodically, evaluate possible risks, and take an action to such risks since vulnerabilities and threats may change in different environments over time.

5. IANA Considerations

This document does not require any IANA actions.

6. Security Considerations

The same security considerations for the I2NSF framework [RFC8329] are applicable to this document.

The development and introduction of I2NSF Analyzer and Security Audit System in the I2NSF Framework may create new security concerns that have to be anticipated at the design and specification time. The usage of machine learning to analyze monitoring data of malicious NSFs may add a risk to its model to be attacked (e.g., adversarial attack) and can result in a bad security policy that is deployed into the I2NSF system.

7. References

7.1. Normative References

[RFC8192] Hares, S., Lopez, D., Zarny, M., Jacquenet, C., Kumar, R., and J. Jeong, "Interface to Network Security Functions (I2NSF): Problem Statement and Use Cases", RFC 8192, DOI 10.17487/RFC8192, July 2017, <https://www.rfc-editor.org/info/rfc8192>.

[RFC8329] Lopez, D., Lopez, E., Dunbar, L., Strassner, J., and R. Kumar, "Framework for Interface to Network Security Functions", RFC 8329, DOI 10.17487/RFC8329, February 2018, <https://www.rfc-editor.org/info/rfc8329>.

[RFC6020] Bjorklund, M., Ed., "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)", RFC 6020, DOI 10.17487/RFC6020, October 2010, <https://www.rfc-editor.org/info/rfc6020>.

[RFC8040] Bierman, A., Bjorklund, M., and K. Watsen, "RESTCONF Protocol", RFC 8040, DOI 10.17487/RFC8040, January 2017, <https://www.rfc-editor.org/info/rfc8040>.

[RFC6241] Enns, R., Ed., Bjorklund, M., Ed., Schoenwaelder, J., Ed., and A. Bierman, Ed., "Network Configuration Protocol (NETCONF)", RFC 6241, DOI 10.17487/RFC6241, June 2011, <https://www.rfc-editor.org/info/rfc6241>.

[I-D.ietf-i2nsf-consumer-facing-interface-dm] Jeong, J. P., Chung, C., Ahn, T., Kumar, R., and S. Hares, "I2NSF Consumer-Facing Interface YANG Data Model", Work in Progress, Internet-Draft, draft-ietf-i2nsf-consumer-facing-interface-dm-31, 15 May 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-i2nsf-consumer-facing-interface-dm-31>.

[I-D.ietf-i2nsf-nsf-facing-interface-dm] Kim, J. T., Jeong, J. P., Jung-Soo, J., Hares, S., and Q. Lin, "I2NSF Network Security Function-Facing Interface YANG Data Model", Work in Progress, Internet-Draft, draft-ietf-i2nsf-nsf-facing-interface-dm-29, 1 June 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-i2nsf-nsf-facing-interface-dm-29>.

[I-D.ietf-i2nsf-registration-interface-dm] Hyun, S., Jeong, J. P., Roh, T., Wi, S., and J. Jung-Soo, "I2NSF Registration Interface YANG Data Model for NSF Capability Registration", Work in Progress, Internet-Draft, draft-ietf-i2nsf-registration-interface-dm-26, 10 May 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-i2nsf-registration-interface-dm-26>.

[I-D.ietf-i2nsf-nsf-monitoring-data-model] Jeong, J. P., Lingga, P., Hares, S., Xia, L., and H. Birkholz, "I2NSF NSF Monitoring Interface YANG Data Model", Work in Progress, Internet-Draft, draft-ietf-i2nsf-nsf-monitoring-data-model-20, 1 June 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-i2nsf-nsf-monitoring-data-model-20>.

7.2. Informative References

[RFC9315] Clemm, A., Ciavaglia, L., Granville, L. Z., and J. Tantsura, "Intent-Based Networking - Concepts and Definitions", RFC 9315, DOI 10.17487/RFC9315, October 2022, <https://www.rfc-editor.org/info/rfc9315>.

[RFC9334] Birkholz, H., Thaler, D., Richardson, M., Smith, N., and W. Pan, "Remote ATtestation procedureS (RATS) Architecture", RFC 9334, DOI 10.17487/RFC9334, January 2023, <https://www.rfc-editor.org/info/rfc9334>.

[I-D.ietf-i2nsf-applicability]
Jeong, J. P., Hyun, S., Ahn, T., Hares, S., and D. Lopez, "Applicability of Interfaces to Network Security Functions to Network-Based Security Services", Work in Progress, Internet-Draft, draft-ietf-i2nsf-applicability-18, 16 September 2019, <https://datatracker.ietf.org/doc/html/draft-ietf-i2nsf-applicability-18>.

[I-D.yang-i2nsf-remote-attestation-interface-dm]
Yang, P., chenmeiling, Su, L., Lopez, D., Jeong, J. P., and L. Dunbar, "I2NSF Remote Attestation Interface YANG Data Model", Work in Progress, Internet-Draft, draft-yang-i2nsf-remote-attestation-interface-dm-01, 5 June 2022, <https://datatracker.ietf.org/doc/html/draft-yang-i2nsf-remote-attestation-interface-dm-01>.

[ICSC] Lingga, P., Jeong, J., and L. Dunbar, "ICSC: Intent-Based Closed-Loop Security Control System for Cloud-Based Security Services", IEEE Communications Magazine, DOI https://doi.org/10.1109/MCOM.001.2400022, December 2024, <https://doi.org/https://doi.org/10.1109/MCOM.001.2400022>.

[SPT] Lingga, P., Jeong, J., Yang, J., and J. Kim, "SPT: Security Policy Translator for Network Security Functions in Cloud-Based Security Services", IEEE Transactions on Dependable and Secure Computing, Volume 21, Issue 6, DOI https://doi.org/10.1109/TDSC.2024.3371788, November 2024, <https://doi.org/https://doi.org/10.1109/TDSC.2024.3371788>.

[ETSI-NFV] "Network Functions Virtualisation (NFV); Architectural Framework", Available: https://www.etsi.org/deliver/etsi_gs/nfv/001_099/002/01.02.01_60/gs_nfv002v010201p.pdf, December 2014.

[Bitcoin] Nakamoto, S., "Bitcoin: A Peer-to-Peer Electronic Cash System", Available: https://bitcoin.org/bitcoin.pdf, May 2009.

[Deep-Learning]
Goodfellow, I., Bengio, Y., and A. Courville, "Deep Learning", The MIT Press, Available: https://www.deeplearningbook.org/, November 2016.

Acknowledgments

This document benefited from discussions in the I2NSF Working Group, especially from Linda Dunbar and Yoav Nir. This document took advantage of the review and comments from the following experts: Qin Wu and Adrian Farrel. The authors sincerely appreciate their sincere efforts and kind help.

This work was supported by Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korea Ministry of Science and ICT (MSIT)(RS-2024-00398199).

This work was supported in part by Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korea Ministry of Science and ICT (MSIT)(No. RS-2022-II221015, Development of Candidate Element Technology for Intelligent 6G Mobile Core Network).

Contributors

The following are coauthors of this document:

Yunchul Choi
Standards & Open Source Research Division
Electronics and Telecommunications Research Institute
218 Gajeong-ro, Yuseong-gu,
Daejeon
34129
Republic of Korea
Email: cyc79@etri.re.kr

Younghan Kim
School of Electronic Engineering
Soongsil University
369, Sangdo-ro, Dongjak-gu
Seoul
06978
Republic of Korea
Email: younghak@ssu.ac.kr

Authors' Addresses

Jaehoon Paul Jeong (editor)
Department of Computer Science and Engineering
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu

Suwon
Gyeonggi-Do
16419
Republic of Korea
Phone: +82 31 299 4957
Email: pauljeong@skku.edu
URI: http://iotlab.skku.edu/people-jaehoon-jeong.php

Patrick Lingga
Department of Electrical and Computer Engineering
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon
Gyeonggi-Do
16419
Republic of Korea
Phone: +82 31 299 4957
Email: patricklink@skku.edu

Jung-Soo Park
Standards & Open Source Research Division
Electronics and Telecommunications Research Institute
218 Gajeong-Ro, Yuseong-Gu
Daejeon
34129
Republic of Korea
Phone: +82 42 860 6514
Email: pjs@etri.re.kr

Diego R. Lopez
Telefonica I+D
Jose Manuel Lara, 9
41013 Seville
Spain
Phone: +34 682 051 091
Email: diego.r.lopez@telefonica.com

Susan Hares
Huawei
7453 Hickory Hill
Saline, MI 48176
United States of America
Phone: +1-734-604-0332
Email: shares@ndzh.com