

Workgroup:

Operations and Management Area Working Group

Internet-Draft:

draft-jeong-opsawg-i2inf-framework-00

Published: 22 July 2024

Intended Status: Informational

Expires: 23 January 2025

Authors: J. Jeong, Ed.

Y. Shen

Sungkyunkwan University

Sungkyunkwan University

Y. Ahn

Y. Kim

Sungkyunkwan University

Soongsil University

E. Duarte Jr.

Federal University of Parana

## **A Framework for Interface to In-Network Functions (I2INF)**

### **Abstract**

This document specifies a framework for Interface to In-Network Functions (I2INF) for a user's services involved in both networks and applications. In-Network Functions (INF) include In-Network Computing Functions (INCF) in Network Functions Virtualization (NFV) and Software-Defined Networking (SDN). They also include In-Network Application Functions (INAF) in Internet-of-Things (IoT) Devices, Software-Defined Vehicles (SDV), and Unmanned Aerial Vehicles (UAV). This document describes an I2INF framework with its components and interfaces to configure and monitor the INFs for the user's services.

### **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 23 January 2025.

### **Copyright Notice**

Copyright (c) 2024 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. Terminology](#)
- [3. A Framework for Interface to In-Network Functions](#)
- [4. Interfaces in the I2INF Framework](#)
- [5. IANA Considerations](#)
- [6. Security Considerations](#)
- [7. References](#)
  - [7.1. Normative References](#)
  - [7.2. Informative References](#)
- [Appendix A. Acknowledgments](#)
- [Appendix B. Contributors](#)
- [Authors' Addresses](#)

## 1. Introduction

Network softwarization is widely deployed for network services in network infrastructure (e.g., 5G mobile networks [[TS-23.501](#)]), clouding computing, and edge computing. The network softwarization is realized by the technologies of Network Functions Virtualization (NFV) [[ETSI-NFV](#)][[ETSI-NFV-Release-2](#)] and Software-Defined Networking (SDN) [[RFC7149](#)]. Also, Intent-Based Networking (IBN) [[RFC9315](#)] [[Survey-IBN-CST-2023](#)] can be used for intelligent network services as well as intelligent application services.

As per definitions of Computing in the Network (COIN), a Programmable Network Device (PND) in an In-Network Computing (INC) environment can have multiple kinds of capabilities (i.e., features) [[I-D.irtf-coinrg-coin-terminology](#)] to work with other PNDs. PNDs from different product lines or vendors can have different capabilities for INC functions. When working together for a COIN system, the PNDs may be unaware of capabilities of others. Therefore, it is necessary to define a standard interface for PNDs to exchange their capabilities.

For the configuration and monitoring of Application Functions (AFs) for applications and Network Functions (NFs) for network services for a given user's service, a standard framework with interfaces is

required. There is no standard data model to describe the capabilities of AFs and NFs for a user-demanded service. Also, there is no standard data model for a registration interface that is used to register the capabilities of those AFs and NFs with a controller for the requested service. In addition, there are no standard interfaces to configure and monitor those AFs and NFs according to a user's intent. Interface to Network Security Functions (I2NSF) was standardized for the control and management of Network Security Services with Network Security Functions (NSFs) [[RFC8329](#)] [[I-D.ietf-i2nsf-applicability](#)]. This document is based on the work of I2NSF for a more general control and management framework for intelligent services consisting of AFs and NFs.

This document specifies a framework for Interface to In-Network Functions (I2INF) for In-Network Functions (INFs) having different capabilities. The INFs consist of Network Functions (NFs) including PNDs and Application Functions (AFs) in order to compose a user's services. First of all, INFs include In-Network Computing Functions (INCF) as NFs within NFV and SDN [[I-D.irtf-coinrg-use-cases](#)]. Secondly, they also include In-Network Application Functions (INAF) as AFs within Internet-of-Things (IoT) Devices, Software-Defined Vehicles (SDV) [[AUTOSAR-SDV](#)][[Eclipse-SDV](#)][[COVESA](#)], and Unmanned Aerial Vehicles (UAV). Finally, this document shows how Intent-Based Networking (IBN) can be realized with the proposed I2INF framework and its interfaces for a user's services consisting of a combination of INFs in a target network.

## 2. Terminology

This document uses the terminology described in [[RFC9315](#)], [[RFC8329](#)], [[I-D.irtf-coinrg-coin-terminology](#)], [[I-D.irtf-coinrg-use-cases](#)], [[I-D.jeong-i2nsf-security-management-automation](#)], [[I-D.jeong-nmrg-ibn-network-management-automation](#)], and [[I-D.yang-i2nsf-security-policy-translation](#)]. In addition, the following terms are defined below:

\*Intent: A set of operational goals (that a network should meet) and outcomes (that a network is supposed to deliver) defined in a declarative manner without specifying how to achieve or implement them [[RFC9315](#)].

\*Intent-Based System (IBS): A system that enforces an intent from a user (or administrator) into a target system (e.g., SDV). An intent can be expressed as a Natural Language (e.g., English) and can be translated into a policy (i.e., network policy and application policy) by a Natural Language Processing (NLP) [[USENIX-ATC-Lumi](#)][[BERT](#)] [[Deep-Learning](#)]. In this document, the intent can be translated into the corresponding high policy by an intent translator

[[I-D.jeong-i2nsf-security-management-automation](#)]. The high-level policy can also be translated into the corresponding low-level policy by a policy translator [[I-D.yang-i2nsf-security-policy-translation](#)]. The low-level policy is dispatched to appropriate Service Functions (SFs). Through the monitoring of the SFs, the activity and performance of the SFs is monitored and analyzed. If needed, the rules of the high-level or low-level network policy are augmented or new rules are generated and configured to appropriate SFs.

\*Mobile Object (MO): An object that is capable of moving by its power source with wireless communication capability such as 5G Vehicle-to-Everything (e.g., 5G V2X). It can be an Internet-of-Things (IoT) device, Software-Defined Vehicle (SDV) [[AUTOSAR-SDV](#)] [[Eclipse-SDV](#)][[COVESA](#)], and Unmanned Aerial Vehicle (UAV). An MO is a Programmable Network Device (PND) [[I-D.irtf-coinrg-coin-terminology](#)] that can be reconfigured for different network requirements inside the MO.

\*In-Network Computing Functions (INCF): The service functions that work for computing in the network infrastructure. They are a group of COIN programs [[I-D.irtf-coinrg-coin-terminology](#)] to provide required computing tasks and functions.

\*In-Network Application Functions (INAF): The service functions that work for applications in Mobile Objects. They are a group of COIN programs [[I-D.irtf-coinrg-coin-terminology](#)] to provide required application tasks and functions.

\*Interface to In-Network Functions (I2INF): Interfaces that are used between a pair of INFs for the interaction for configuration and monitoring.

\*A Framework for Interface to In-Network Functions (I2INF): a framework that consists of components and interfaces to configure and monitor INFs for various services in the network infrastructure and MOs.

### **3. A Framework for Interface to In-Network Functions**

This section specifies a framework for Interface to In-Network Functions (I2INF) with its components and interfaces among the components. [Figure 1](#) shows Wireless and Wired Networks in a Central Cloud for the I2INF framework having network entities and Mobile Objects (MO). On the other hand, [Figure 2](#) shows a VNF-Consensus Architecture in an Edge Cloud for the I2INF framework to synchronize the SDN Controllers for flow table information in the same Edge Cloud [[NFV-COIN](#)].



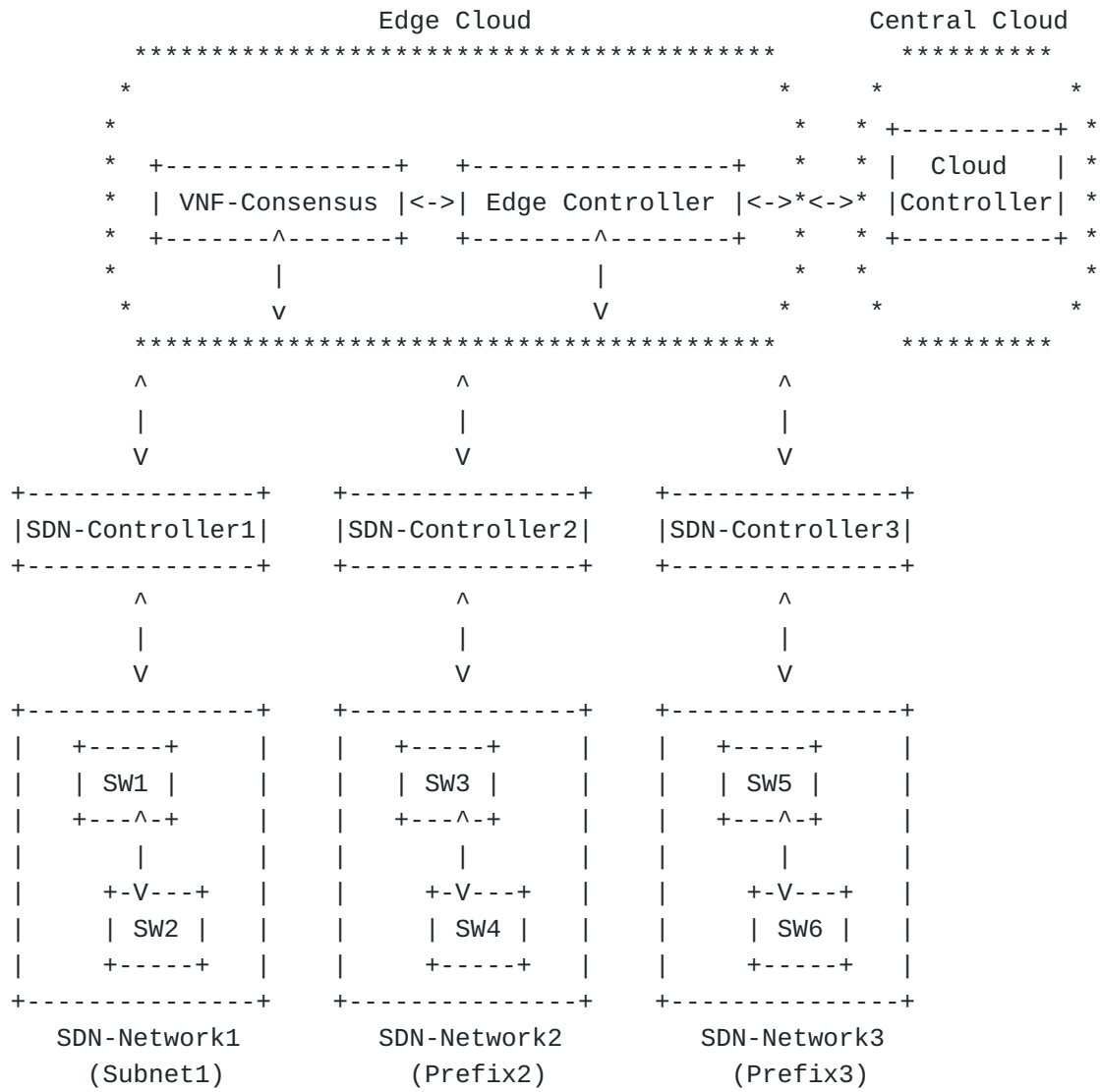


Figure 2: VNF-Consensus Architecture in Edge Cloud for I2INF Framework

For the automatic network configuration of MOs, an intent-based management is required between the central cloud and MOs [I-D.jeong-nmrg-ibn-network-management-automation]. Figure 3 shows an I2INF framework as an IBS for an MO. The framework consists of a Central Cloud and an MO. Figure 4 shows an I2INF framework as an IBS for an Edge Cloud. The framework consists of a Central Cloud and an Edge Cloud.

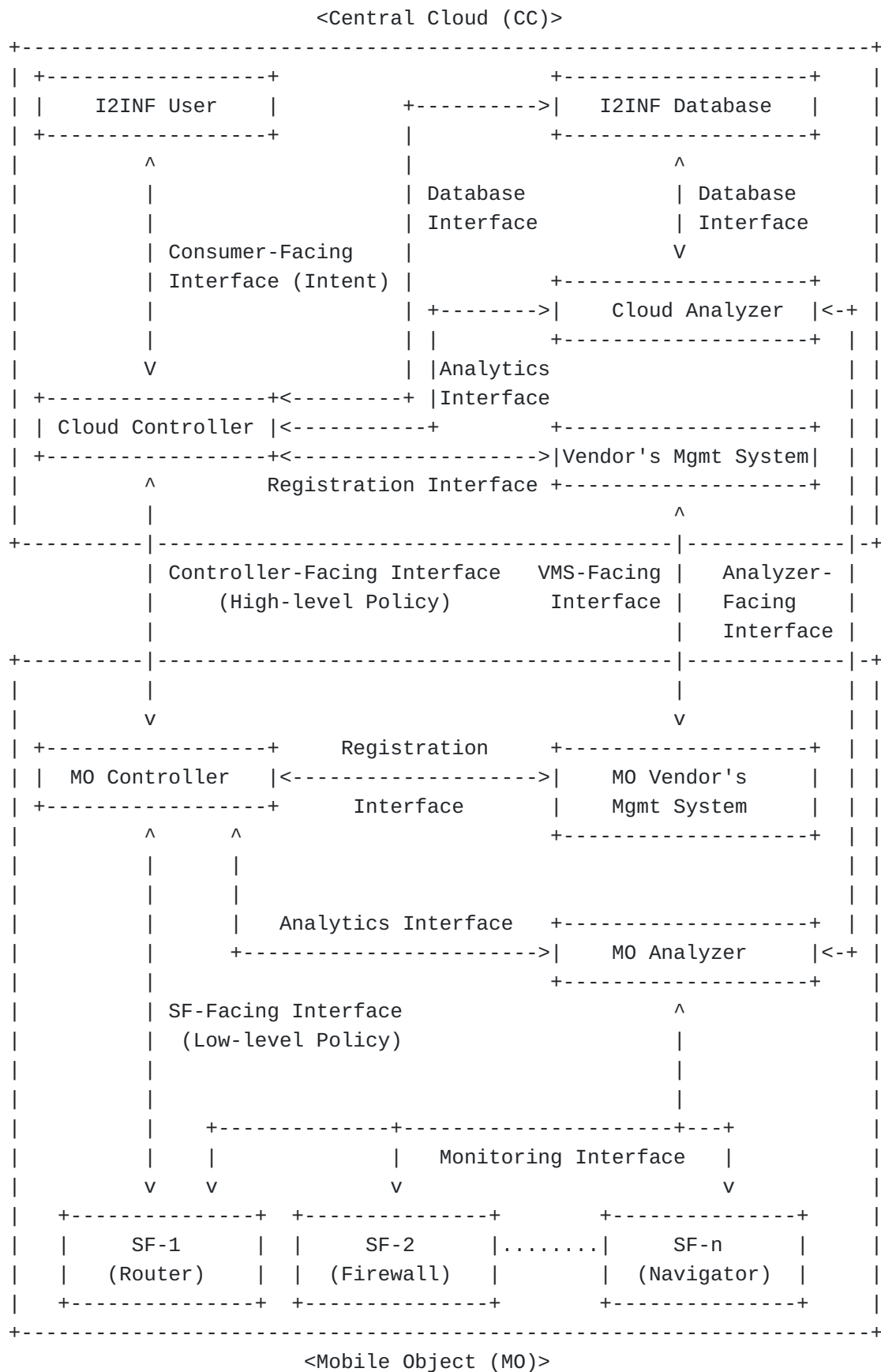


Figure 3: A Framework for Interface to In-Network Functions for Mobile  
Object



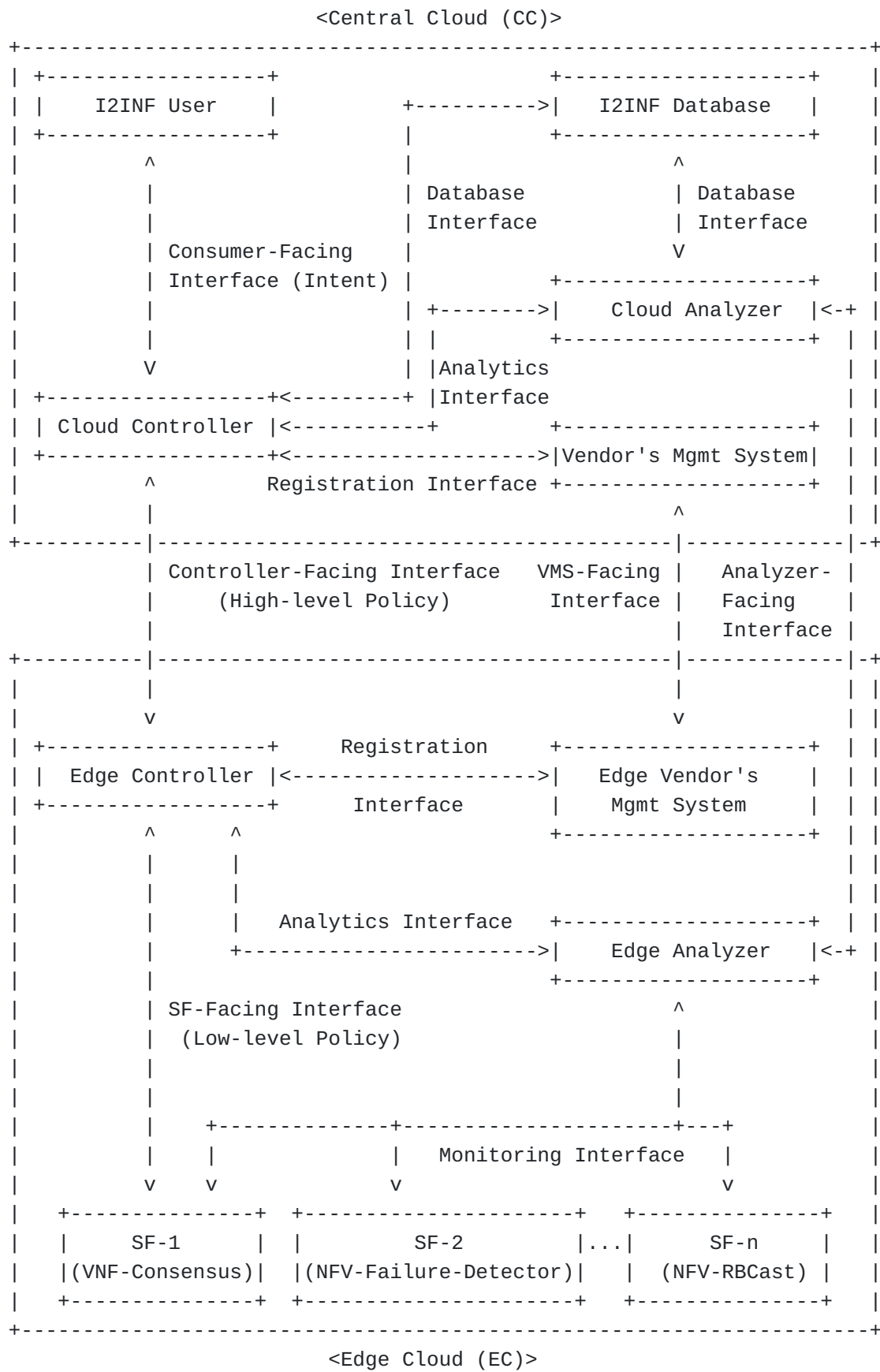


Figure 4: A Framework for Interface to In-Network Functions for Edge Cloud

A Central Cloud (CC) consists of I2INF User (as network administrator), Cloud Controller (as an orchestrator for a central cloud), I2INF Database (as a main repository for INF management and monitoring), and Cloud Analyzer (as a monitoring data analyzer for MOs and ECs) such as Network Data Analytics Function (NWDAF) in 5G networks [[TS-23.288](#)][[TS-29.520](#)].

\*I2INF User: It is the software (e.g., web-browser-based user interface) used by I2INF administrators to deliver network intents to MO controllers and edge controller. In the 3GPP intent-driven management service document, it is assumed that a network intent is configured by an intent data model [[TS-28.312](#)] [[TR-28.812](#)].

\*Cloud Controller: It is a component that controls and manages other system components of the central cloud. From a security point of view, a security service policy can be transmitted to the service function (SF) by converting the I2INF User's security service intent into the corresponding security service policy and selecting an SF that provides an appropriate security service.

\*Cloud Vendor's Management System: It is a component that provides images of virtualized SFs for cloud services and registers the SFs and access information with Cloud Controller.

\*Cloud Analyzer: It gathers and evaluates monitoring data from MO Analyzers and Edge Analyzers to ensure the functionality and performance of SFs, e.g., the network data analytics function (NWDAF) in 5G networks.

\*I2INF Database: It is a database for managing MOs and ECs, including network and security configuration and status of MOs and ECs. For example, for MOs, it maintains the current locations and navigation paths of MOs (e.g., SDVs). For ECs, it maintains the network configuration and status of AFs and NFs within the edge cloud.

An IBS in an MO (or EC) is composed of MO Controller (or Edge Controller) as a manager for the MO (or EC), MO Analyzer (or Edge Analyzer) as a monitoring data analyzer for an MO (or EC) [[I-D.jeong-nmrg-ibn-network-management-automation](#)], Vendor's Management System (as a vendor system to provide cloud-native containers) [[RFC8329](#)], and Service Functions (SFs). As SFs for the MO, NFs include router, DNS server, and firewall [[I-D.jeong-nmrg-ibn-network-management-automation](#)]), and AFs include safe driver and navigator. As SFs for the EC, NFs include VNF-Consensus, NFV-Failure-Detector, and NFV-RBCast (i.e., NFV Reliable-

Ordered Broadcast) [[NFV-COIN](#)]). The functions of each component is described as follows.

\*MO Controller: It is a component that controls and manages other components of the MO framework (or EC framework). It translates the high-level policy received from the Cloud Controller into a low-level policy that the SF can understand. An SF to perform this low-level service policy is selected, and the policy is transmitted to the SF.

\*MO Vendor's Management System (or Edge Vendor's Management System): It is a component that provides an image of a virtualized SF for MO services (or EC services) to the MO framework (or EC framework) and registers the function and access information of the SF with MO Controller (or Edge Controller).

\*Service Function (SF): It is a component that refers to a virtual network function (VNF), cloud native network function (CNF), or physical network function (PNF) for a specific service. For security services, it provides security services such as firewalls, web filters, DDoS attack mitigators, and anti-viruses. In addition, networks and application services can also operate as SFs.

\*MO Analyzer (or Edge Analyzer): It is a component that collects monitoring data from SFs of MOs (or ECs) and analyzes these data to confirm the activity and performance of SFs. MO Analyzer (or Edge Analyzer) acts as NWDAF in a 5G network. If there are problems (e.g., security attacks, traffic congestion, QoS degradation) in the MO's internal network (or EC's internet network), MO Analyzer (or Edge Analyzer) delivers either policy reconfiguration or feedback information to MO Controller (or Edge Controller) for security and network troubleshooting.

#### **4. Interfaces in the I2INF Framework**

Together with the designed I2INF framework, in [Figure 3](#) and [Figure 4](#), interfaces are also defined between a pair of system components in the central cloud and MO (or EC), respectively. These interfaces include

\*Consumer-Facing Interface: It is an interface between I2INF User and Cloud Controller for conveying intents.

\*Controller-Facing Interface: It is an interface between Cloud Controller and MO Controller (or Edge Controller) for high-level policy delivery with translated intents.

\*SF-Facing Interface: It is an interface between MO Controller (or Edge Controller) and SF for the delivery of a translated lower-level policy.

\*Registration Interface: It is an interface used to transfer SF capabilities and access information for registration to either Cloud Controller or MO Controller (or Edge Controller), or deliver SF queries for searching the requested SFs. For an MO, this interface can be an interface between Cloud Controller and Cloud Vendor's Management System (Cloud VMS), or between MO Controller and MO Vendor's Management System (MO VMS). Also, for an EC, this interface can be an interface between Cloud Controller and Cloud Vendor's Management System (Cloud VMS), or between Edge Controller and Edge Vendor's Management System (Edge VMS).

\*Monitoring Interface: It is an interface between the SF and the MO Analyzer (or Edge Analyzer) used to collect the SF's monitoring data to identify SF-related security, system, and network issues.

\*Analytics Interface: It is an interface for delivering policy reconfiguration or feedback as a result of analyzing SF monitoring data. For an MO, this interface is an interface between MO Analyzer and MO Controller, or between Cloud Analyzer and Cloud Controller. Also, for an EC, this interface is an interface between Edge Analyzer and Edge Controller, or between Cloud Analyzer and Cloud Controller.

\*Analyzer-Facing Interface: It is an interface between MO Analyzer (or Edge Analyzer) and Cloud Analyzer for the exchange of security, network, and system-related analysis of SFs.

\*VMS-Facing Interface: It is an interface between Cloud VMS and MO VMS (or Edge VMS) to exchange SF container images with SF feature information.

\*Database Interface: It is an interface for exchanging data in an I2INF database. It is an interface between I2INF Database and Cloud Controller, or between I2INF Database and Cloud Analyzer.

The intent, high-level policy, and low-level policy can be either XML documents [[RFC6020](#)][[RFC7950](#)] or YAML documents [[YAML](#)]. They can be delivered to the destination components via NETCONF [[RFC6241](#)], RESTCONF [[RFC8040](#)], or REST API [[REST](#)].

As shown in [Figure 3](#) and [Figure 4](#), the I2INF Framework enforces an intent from an I2INF User, which as a user (or administrator), into a target system such as an MO (e.g., SDV) and an Edge Cloud. The intent from the I2INF User can be translated into the corresponding high-level policy by an intent translator in the Cloud Controller of the Central Cloud [[I-D.jeong-i2nsf-security-management-automation](#)]. The

high-level policy can also be translated into the corresponding low-level policy by a policy translator in the MO Controller of the MO or the Edge Controller of the Edge Cloud

[[I-D.yang-i2nsf-security-policy-translation](#)]. For the MO, as shown in [Figure 3](#), the low-level policy is dispatched from the MO Controller to appropriate Service Functions (SFs) in the MO, such as Router, Firewall, and Navigator. Also, for the EC, as shown in [Figure 4](#), the low-level policy is dispatched from the Edge Controller to appropriate Service Functions (SFs) in the EC, such as VNF-Consensus, NFV-Failure-Detector, and NFV-RBCast. Through the monitoring of the SFs, the activity and performance of the SFs in the MO (or EC) is monitored and analyzed by the MO Analyzer (or Edge Analyzer) in the MO (or EC). If needed, the rules of the high-level or low-level network policy can be augmented by the MO Analyzer (or Edge Analyzer). Also, new rules can be automatically generated and configured to appropriate SFs by the MO Analyzer (or Edge Analyzer).

Therefore, this document proposes an I2INF framework as an IBS for both MOs and ECs. Through this IBS, the SFs (i.e., NFs and AFs) in the MOs and ECs can be better configured and managed. Base on the proposed framework, both virtualized NFs and AFs can be efficiently orchestrated for agile resource re-configurations and flexible updates.

## 5. IANA Considerations

This document does not require any IANA actions.

## 6. Security Considerations

The same security considerations for the Interface to Network Security Functions (I2NSF) Framework [[RFC8329](#)] are applicable to the Intent-Based System this document.

## 7. References

### 7.1. Normative References

- [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>>.
- [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>>.
- [RFC7149] Boucadair, M. and C. Jacquenet, "Software-Defined Networking: A Perspective from within a Service Provider

Environment", RFC 7149, DOI 10.17487/RFC7149, March 2014, <<https://www.rfc-editor.org/info/rfc7149>>.

[RFC7950] Bjorklund, M., Ed., "The YANG 1.1 Data Modeling Language", RFC 7950, DOI 10.17487/RFC7950, August 2016, <<https://www.rfc-editor.org/info/rfc7950>>.

[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>>.

[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>>.

[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>>.

[RFC9365] Jeong, J., Ed., "IPv6 Wireless Access in Vehicular Environments (IPWAVE): Problem Statement and Use Cases", RFC 9365, DOI 10.17487/RFC9365, March 2023, <<https://www.rfc-editor.org/info/rfc9365>>.

## 7.2. Informative References

[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.irtf-coinrg-coin-terminology] Hong, J., Kunze, I., Wehrle, K., Trossen, D., Montpetit, M., de Foy, X., Griffin, D., and M. Rio, "Terminology for Computing in the Network", Work in Progress, Internet-Draft, draft-irtf-coinrg-coin-terminology-01, 10 July 2023, <<https://datatracker.ietf.org/doc/html/draft-irtf-coinrg-coin-terminology-01>>.

[I-D.irtf-coinrg-use-cases] Kunze, I., Wehrle, K., Trossen, D., Montpetit, M., de Foy, X., Griffin, D., and M. Rio, "Use Cases for In-Network Computing", Work in Progress, Internet-Draft, draft-irtf-coinrg-use-cases-05, 23 February 2024, <<https://>

[datatracker.ietf.org/doc/html/draft-irtf-coinrg-use-cases-05](https://datatracker.ietf.org/doc/html/draft-irtf-coinrg-use-cases-05)>.

**[I-D.ietf-i2nsf-capability-data-model]** Hares, S., Jeong, J. P., Kim, J. T., Moskowitz, R., and Q. Lin, "I2NSF Capability YANG Data Model", Work in Progress, Internet-Draft, draft-ietf-i2nsf-capability-data-model-32, 23 May 2022, <<https://datatracker.ietf.org/doc/html/draft-ietf-i2nsf-capability-data-model-32>>.

**[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-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-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>>.

**[I-D.lingga-i2nsf-analytics-interface-dm]** Lingga, P., Jeong, J. P., and Y. Choi, "I2NSF Analytics Interface YANG Data Model", Work in Progress, Internet-Draft, draft-lingga-i2nsf-analytics-interface-dm-03, 7 February 2024, <<https://datatracker.ietf.org/doc/html/draft-lingga-i2nsf-analytics-interface-dm-03>>.

**[I-D.jeong-i2nsf-security-management-automation]**

Jeong, J. P., Lingga, P., Jung-Soo, J., Lopez, D., and S. Hares, "Security Management Automation of Cloud-Based Security Services in I2NSF Framework", Work in Progress, Internet-Draft, draft-jeong-i2nsf-security-management-automation-07, 7 February 2024, <<https://datatracker.ietf.org/doc/html/draft-jeong-i2nsf-security-management-automation-07>>.

**[I-D.jeong-nmrg-ibn-network-management-automation]**

Jeong, J. P., Ahn, Y., Kim, Y., and J. Jung-Soo, "Intent-Based Network Management Automation in 5G Networks", Work in Progress, Internet-Draft, draft-jeong-nmrg-ibn-network-management-automation-04, 22 April 2024, <<https://datatracker.ietf.org/doc/html/draft-jeong-nmrg-ibn-network-management-automation-04>>.

**[I-D.yang-i2nsf-security-policy-translation]**

Jeong, J. P., Lingga, P., and J. Yang, "Guidelines for Security Policy Translation in Interface to Network Security Functions", Work in Progress, Internet-Draft, draft-yang-i2nsf-security-policy-translation-16, 7 February 2024, <<https://datatracker.ietf.org/doc/html/draft-yang-i2nsf-security-policy-translation-16>>.

**[YAML]**

Ingerson, B., Evans, C., and O. Ben-Kiki, "Yet Another Markup Language (YAML) 1.0", Available: <https://yaml.org/spec/history/2001-05-26.html>, October 2023.

**[TS-23.501]**

"System Architecture for the 5G System (5GS)", Available: <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144>, September 2023.

**[TS-28.312]**

"Intent Driven Management Services for Mobile Networks", Available: <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3554>, September 2023.

**[TR-28.812]**

"Study on Scenarios for Intent Driven Management Services for Mobile Networks", Available: <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3553>, December 2020.

**[TS-23.288]**

"Architecture Enhancements for 5G System (5GS) to Support Network Data Analytics Services", Available: <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3579>, September 2023.



**[TS-29.520]**

"Network Data Analytics Services", Available: <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3355>, September 2023.

**[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](https://www.etsi.org/deliver/etsi_gs/nfv/001_099/002/01.02.01_60/gs_nfv002v010201p.pdf), December 2014.

**[ETSI-NFV-Release-2]**

"Network Functions Virtualisation (NFV) Release 2; Management and Orchestration; Architectural Framework Specification", Available: [https://www.etsi.org/deliver/etsi\\_gs/nfv/001\\_099/006/02.01.01\\_60/gs\\_nfv006v020101p.pdf](https://www.etsi.org/deliver/etsi_gs/nfv/001_099/006/02.01.01_60/gs_nfv006v020101p.pdf), January 2021.

**[NFV-COIN]**

Venancio, G., Turchetti, R., and E. Duarte Jr., "NFV-COIN: Unleashing The Power of In-Network Computing with Virtualization Technologies", SBC Journal of Internet Services and Applications, Available: <https://journals-sol.sbc.org.br/index.php/jisa/article/view/2342>, December 2022.

**[REST]**

Fielding, R. and R. Taylor, "Principled Design of the Modern Web Architecture", ACM Transactions on Internet Technology, Vol. 2, Issue 2,, Available: <https://dl.acm.org/doi/10.1145/514183.514185>, May 2002.

**[USENIX-ATC-Lumi]**

Jacobs, A., Pfitscher, R., Ribeiro, R., Ferreira, R., Granville, L., Willinger, W., and S. Rao, "Hey, Lumi! Using Natural Language for Intent-Based Network Management", USENIX Annual Technical Conference, Available: <https://www.usenix.org/conference/atc21/presentation/jacobs>, July 2021.

**[BERT]**

Devlin, J., Chang, M., Lee, K., and K. Toutanova, "BERT: Pre-training of Deep Bidirectional Transformers for

Language Understanding", NAACL-HLT Conference, Available: <https://aclanthology.org/N19-1423.pdf>, June 2019.

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

**[AUTOSAR-SDV]** "AUTOSAR Adaptive Platform", Available: <https://www.autosar.org/standards/adaptive-platform>, March 2024.

**[Eclipse-SDV]** "Eclipse Software Defined Vehicle Working Group Charter", Available: <https://www.eclipse.org/org/workinggroups/sdv-charter.php>, March 2024.

**[COVESA]** "Connected Vehicle Systems Alliance", Available: <https://covesa.global/>, March 2024.

**[Kubernetes]** "Kubernetes: Cloud Native Computing Platform", Available: <https://kubernetes.io/>, March 2024.

**[Survey-IBN-CST-2023]** Leivadeas, A. and M. Falkner, "A Survey on Intent-Based Networking", Available: <https://ieeexplore.ieee.org/document/9925251>, March 2023.

## **Appendix A. Acknowledgments**

This work was supported by Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korea Ministry of Science and ICT (MSIT) (No. 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. 2022-0-01015, Development of Candidate Element Technology for Intelligent 6G Mobile Core Network).

## **Appendix B. Contributors**

This document is made by the group effort of OPWAWG, greatly benefiting from inputs and texts by Linda Dunbar (Futurewei), Yong-Geun Hong (Daejeon University), and Joo-Sang Youn (Dong-Eui University). The authors sincerely appreciate their contributions.

The following are coauthors of this document:

Mose Gu  
Department of Computer Science & Engineering  
Sungkyunkwan University  
2066 Seobu-Ro, Jangan-Gu  
Suwon

Gyeonggi-Do  
16419  
Republic of Korea

Phone: [+82 31 299 4106](tel:+82-31-299-4106)  
Email: [rna0415@skku.edu](mailto:rna0415@skku.edu)  
URI: <http://iotlab.skku.edu/people-Moses-Gu.php>

Juwon Hong  
Department of Computer Science & Engineering  
Sungkyunkwan University  
2066 Seobu-Ro, Jangan-Gu  
Suwon  
Gyeonggi-Do  
16419  
Republic of Korea

Phone: [+82 31 299 4106](tel:+82-31-299-4106)  
Email: [hongju2024@skku.edu](mailto:hongju2024@skku.edu)  
URI: <http://iotlab.skku.edu/people-Joo-Won-Hong.php>

#### 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](tel:+82-31-299-4957)  
Email: [pauljeong@skku.edu](mailto:pauljeong@skku.edu)  
URI: <http://iotlab.skku.edu/people-jaehoon-jeong.php>

Yiwen Shen  
Department of Computer Science and Engineering  
Sungkyunkwan University  
2066 Seobu-Ro, Jangan-Gu  
Suwon  
Gyeonggi-Do  
16419  
Republic of Korea

Phone: [+82 31 299 4106](tel:+82-31-299-4106)  
Email: [chrisshen@skku.edu](mailto:chrisshen@skku.edu)  
URI: <https://chrisshen.github.io>

Yoseop Ahn

Department of Computer Science and Engineering  
Sungkyunkwan University  
2066 Seobu-Ro, Jangan-Gu  
Suwon  
Gyeonggi-Do  
16419  
Republic of Korea

Phone: [+82 31 299 4106](tel:+82-31-299-4106)

Email: [ahnjs124@skku.edu](mailto:ahnjs124@skku.edu)

URI: <http://iotlab.skku.edu/people-Ahn-Yoseop.php>

Younghan Kim  
School of Electronic Engineering  
Soongsil University  
369, Sangdo-ro, Dongjak-gu  
Seoul  
06978  
Republic of Korea

Email: [younghak@ssu.ac.kr](mailto:younghak@ssu.ac.kr)

Elias P. Duarte Jr.  
Department of Computer Science and Engineering  
Federal University of Parana  
Brazil

Email: [elias@inf.ufpr.br](mailto:elias@inf.ufpr.br)