Operations and Management Area Working Group
Internet-Draft
Intended status: Informational
Expires: 8 January 2026

Y. Ahn, Ed.
J. Jeong, Ed.
Sungkyunkwan University
Y. Kim
Soongsil University

7 July 2025

An Integrated Security Service System for 5G Networks using an I2NSF Framework
draft-ahn-opsawg-5g-security-i2nsf-framework-00

Abstract

This document presents an integrated framework for automated security management in 5G edge networks using the Interface to Network Security Functions (I2NSF) architecture. The proposed system leverages Intent-Based Networking (IBN) to allow users or administrators to declare high-level security intents, which are then translated into enforceable network and application policies. Network-level policies are delivered to 5G core components via the Network Exposure Function (NEF), while application-level policies are enforced directly at user equipment through distributed IBN Controllers. This architecture supports adaptive, context-aware, and distributed policy enforcement, enabling real-time response to dynamic edge conditions and user mobility scenarios such as handovers. By integrating closed-loop monitoring and analytics, the system ensures consistent and autonomous security across heterogeneous 5G environments.

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 8 January 2026.

Table of Contents

1. Introduction

Network softwarization has become a fundamental approach for delivering network services across various infrastructures, including 5G mobile networks [TS-23.501], cloud computing platforms, and edge computing environments. This paradigm is enabled through key technologies such as Network Functions Virtualization (NFV) [ETSI-NFV] and Software-Defined Networking (SDN) [RFC7149]. In addition, Intent-Based Networking (IBN) [RFC9315] [Survey-IBN-CST-2023] serves as a foundation for implementing intelligent behaviors in both network-level and application-level services. As networks continue to evolve in this software-driven direction, the emergence of 5G introduces new challenges, particularly in the realm of security.

As mobile networks evolve toward 5G, the increasing complexity of network functions and the widespread deployment of edge devices such as IoT nodes, user equipment (UE), and application functions (AFs)

[TS-23.501] introduce significant challenges to existing security models. These environments are inherently dynamic, heterogeneous, and latency-sensitive, making it difficult for traditional rule-based configurations, which are typically static and manually managed, to respond effectively to changing conditions. In particular, security operations at the edge require more contextual awareness, automation, and adaptability than ever before.

Intent-Based Networking (IBN) provides a promising paradigm to meet these requirements. It enables operators or users to declare high-level goals, or intents, which the system can automatically translate into enforceable security and network policies [TS-28.312]. These policies may range from abstract service-level objectives to fine-grained access control rules. By automating this translation and enforcement process, the network gains the ability to respond autonomously to operational demands without requiring manual intervention. This model supports closed-loop control, where real-time feedback mechanisms continuously refine and adapt system behavior based on evolving context and intent.

This document defines an intent-based framework for edge security management in the context of 5G systems. The framework builds upon the service-based architecture (SBA) defined in 3GPP 5G and beyond, and introduces a layered approach that includes intent translation, policy generation, enforcement, and monitoring. It integrates seamlessly with existing 3GPP network functions such as the Policy Control Function (PCF) [TS-29.520], Access and Mobility Management Function (AMF), Session Management Function (SMF), and Network Data Analytics Function (NWDAF) [TS-23.288]. The aim is to deliver scalable and adaptive security control across heterogeneous edge domains through policy-driven orchestration.

Furthermore, the framework is designed to support mobility scenarios, including handovers between gNBs and session migration across multiple User Plane Functions (UPFs). By dynamically enforcing intents at the edge, the system maintains consistent and context-aware security postures even in the presence of mobility events. This capability strengthens the resilience and responsiveness of the network while laying a foundation for secure, automated, and intelligent 5G services. The proposed framework also aligns with long-term goals of zero-touch security, AI-driven orchestration, and intent-based policy automation within future mobile network infrastructures.

2. Terminology

This section provides definitions of the key terms and concepts used throughout this document. The terminology is intended to establish a common understanding of the architectural elements, interfaces, and operational principles discussed in the context of intent-based security management in 5G networks. These terms are used to describe 5G Network automation based on the Intent-Based Networking (IBN) and Interface to Network Security Functions (I2NSF) framework.

* Intent: It refers to a set of operational objectives and expected outcomes that a network should fulfill, expressed in a declarative manner without specifying the implementation details or the exact procedures to achieve them [RFC9315]. Intents can be represented using XML [RFC6020] [RFC7950] or YAML [YAML] formats, and may be delivered to the target components through protocols such as NETCONF [RFC6241], RESTCONF [RFC8040], or via standard REST APIs [REST].

* IBN User Function (IUF): It is typically accessed via a web-browser interface, which allows Mobile Object administrators to input network intents for the IBN Control Function (ICF). These intents serve as strategic objectives that guide the generation of security and network policies within the system.

* IBN Control Function (ICF): The ICF operates as a core component of the I2NSF architecture deployed within the 5G network. It is responsible for managing and orchestrating security enforcement functions by translating the intents from the IUF into actionable policies, and by selecting appropriate 5G Network Functions (NFs) for their execution.

* Developer’s Management Function (DMF): It is a component within the Interface to Network Security Functions (I2NSF) framework that acts as a provider of Network Security Functions (NSFs). It’s responsible for registering the capabilities of these NSFs with the Security Controller, essentially making them available for use in enforcing security policies.

* Security Control Function (SCF): SCF strengthens network security by generating low-level policies to modify and supplement the network configuration based on the delivered network policy and delivering these to the relevant individual NFs.

* Security Data Analytics Function (SDAF): It collects and analyzes monitoring data to verify whether the policies generated based on intents have been properly enforced by the network security functions, and to evaluate the performance and functionality of the security services.

* Network Security Function (NSF): NSF is a network security function that provides actual security services based on policies generated based on the user's intent. It actually executes security tasks such as blocking or allowing traffic based on the policy delivered from ICF.

3. An I2NSF-Based Architecture for 5G Edge Security Management

This section defines a comprehensive framework for 5G security management automation by introducing its essential components and explaining how each of them is designed to interconnect with functions in the 5G core networks [TS-23.501]. The framework is grounded in intent-based networking principles, which enable high-level user or application intents to be automatically translated into actionable policies. These policies are then enforced and monitored across both the core and edge domains without requiring manual intervention.

As 5G networks become more distributed and support a growing number of latency-sensitive services and heterogeneous devices, traditional static security mechanisms struggle to cope with the dynamic nature of threats and the scale of real-time traffic. Manual configuration is no longer feasible in such environments, making automated security orchestration essential to maintain consistent protection, reduce response time, and minimize human error.

To realize this, the framework leverages a set of I2NSF-based functional modules that collectively support policy translation, enforcement, and real-time monitoring. By integrating these components into the 5G architecture, the system enables scalable, adaptive, and context-aware security operations tailored to the needs of dynamic and heterogeneous edge environments.

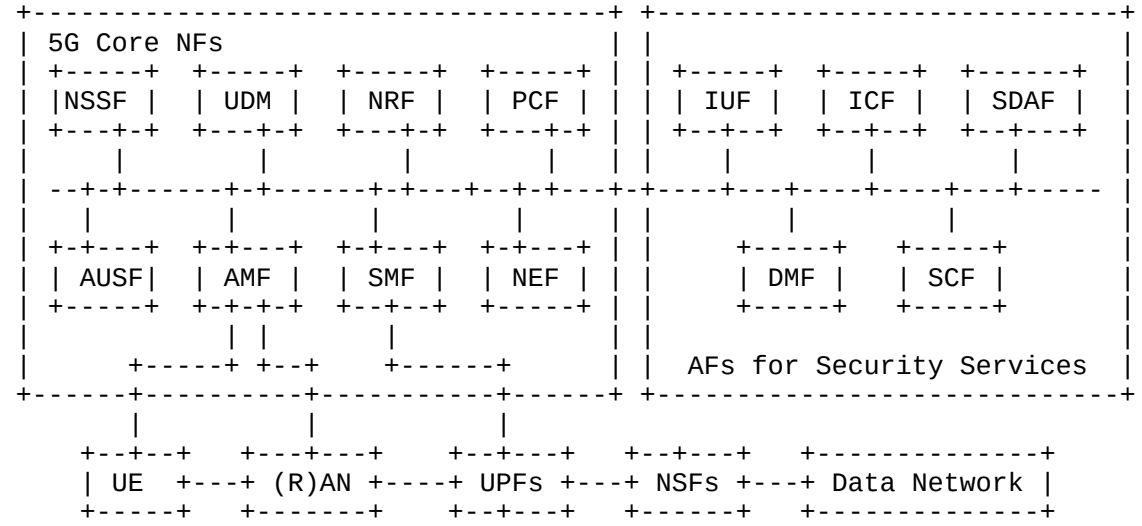


Figure 1: I2NSF-Based Security Management Framework for 5G Edge Networks

Figure 1 illustrates a 5G edge security service architecture based on the I2NSF framework [RFC8329], implemented as an Intent-Based System (IBS). An intent-based management strategy is required between the 5G Core network and distributed edge domains to enable the autonomous configuration and security enforcement of edge functions such as User Equipment (UEs), as described in the IETF draft on intent-based network management automation.

On the right side of the architecture, the AFs for Security Services represent application-layer functions that initiate and manage high-level security intents. These functions serve as the interface between external users or applications and the intent-based security system. This service is composed of several key modules, including the Intent-Based Use Function (IUF), the Intent Control Function (ICF), the Security Control Function (SCF), the Developer’s Management Function (DMF), and the Security Data Analytics Function (SDAF), which collectively support intent interpretation, policy translation, enforcement, and monitoring across the network.

The security intent generated by the Intent-Based Network Use Function (IUF) is first interpreted as a high-level objective reflecting the desired behavior of the network or specific applications. This intent is then processed by the Intent-Based Network Control Function (ICF), which plays a central role in translating the abstract intent into concrete policies. Through this translation process, two distinct types of policies are created: a

network policy, which governs how the underlying network should behave (e.g., traffic routing, filtering, or QoS enforcement), and an application policy, which defines how specific applications or devices should operate under given security constraints.

Once these policies are generated, they are delivered to the 5G Core Network via the Network Exposure Function (NEF). The NEF serves as the gateway between external application functions and the internal control plane of the 5G Core. To support flexible deployment and orchestration, these components can be implemented as containerized microservices and managed using Kubernetes[Kubernetes]. By passing the policies through the NEF, the system enables relevant 5G Core components such as the Policy Control Function (PCF), Session Management Function (SMF), and Access and Mobility Management Function (AMF) to enforce the translated policies in real time. This ensures that the original user or service intent is consistently and dynamically applied throughout the network.

4. The Procedure for I2NSF-Based 5G Edge Security Management

This testbed demonstrates a use case where high-level user intents are automatically translated into enforceable network and application policies. Leveraging the I2NSF (Interface to Network Security Functions) framework [RFC8329] and deployed on the free5GC platform, this architecture enables automated, intent-driven security management that reduces the reliance on manual configuration and static rule sets.

The system is designed to support distributed policy enforcement by integrating key I2NSF components such as the Intent-Based Networking Use Function (IUF), Intent Control Function (ICF), Security Control Function (SCF), and Security Data Analytics Function (SDAF). These components work collaboratively to process intents, generate appropriate policies, and enforce them dynamically across both the core network and the edge.

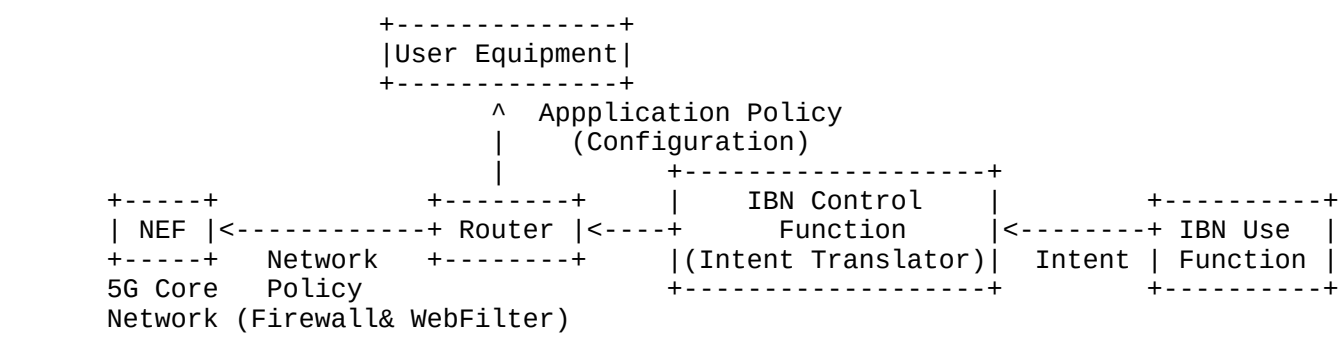
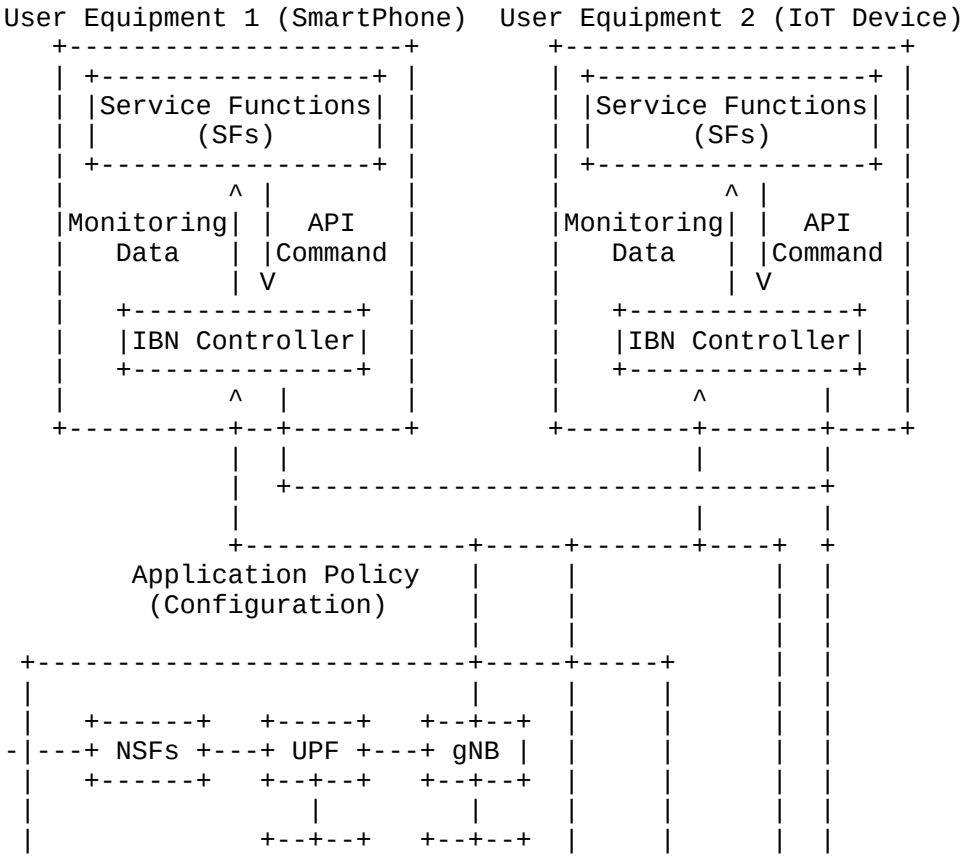


Figure 2: The Procedure of Policy Generation and Delivery for 5G Edge Network

Figure 2 shows the procedure for 5G Edge Security Management Automation, specifically illustrating the creation of user intents and the generation of corresponding network policies and application policies. The process begins when a user or administrator expresses a security-related intent via the IBN Use Function (IUF). This intent, representing a high-level goal such as restricting access to certain websites or monitoring device behavior, is passed to the IBN Control Function (ICF). The ICF, equipped with an Intent Translator, converts this intent into both network-level and application-level policies. The translated network-level policies are forwarded through the router to the 5G Core's Network Exposure Function (NEF) [TS-29.503], while the application-level policies are delivered directly to the User Equipment (UE). This enables consistent policy enforcement from the core network to the device edge.



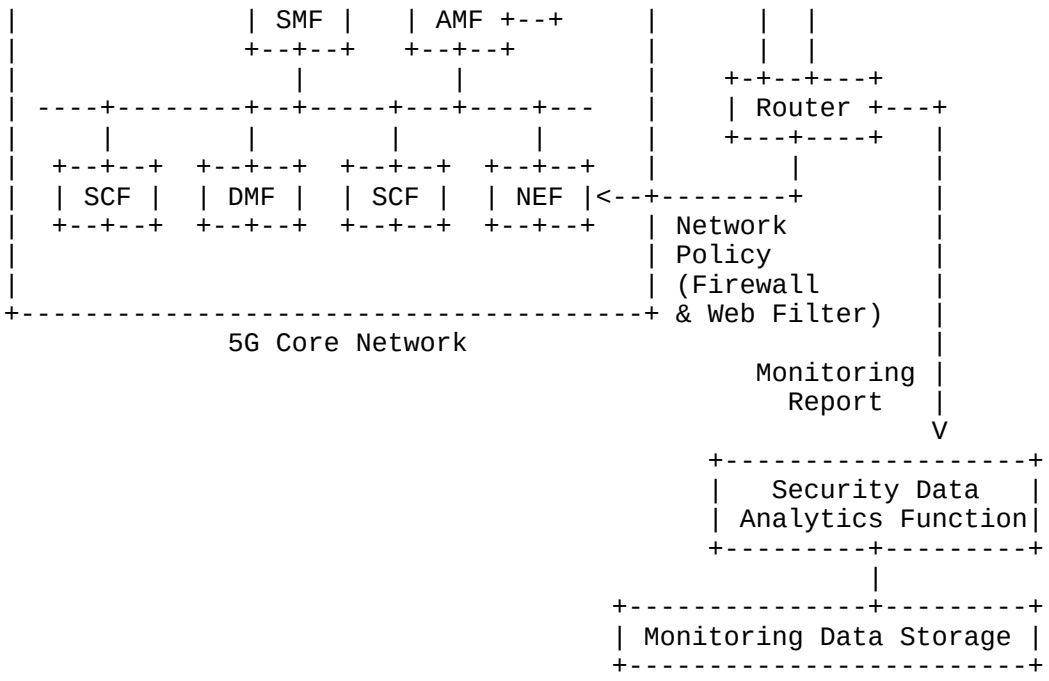


Figure 3: The Procedure within an I2NSF-Based Framework for 5G Edge Security Management

Figure 3 illustrates the procedure of how the intent-driven network policies and application policies are applied across both the 5G core network and user equipment. These policies are then propagated throughout the 5G network to support coordinated and consistent security enforcement. Network-level policies are distributed to core network functions [TS-23.501], where they help guide the overall behavior and resource allocation of the system in alignment with the user's intent. At the same time, application-level policies are delivered to various user devices, such as smartphones and IoT nodes, which have embedded controllers capable of interpreting and enforcing the received policies locally.

This allows each device to autonomously adjust its behavior according to the defined security or operational requirements. In parallel, network-based security functions are also engaged to apply the necessary controls, such as access restrictions or traffic filtering, ensuring that both the core and the edge of the network operate securely and in harmony with the original intent. This distributed approach enables flexible, scalable, and adaptive policy enforcement across the entire mobile network environment [TS-23.288].

To support adaptive security validation, each user equipment's IBN Controller periodically generates monitoring reports based on local policy enforcement status. These reports are sent to the Security Data Analytics Function (SDAF), which analyzes the monitoring data to evaluate whether the applied policies are effectively enforced. All collected data is stored in a centralized Monitoring Data Storage module, enabling real-time policy validation and historical auditing. The related steps are as follows:

* Steps 1-2: An intent is sent from an application within the 5G Core to the IBN Control Function, where it is translated into network and application policies. This marks the beginning of intent-driven automation for security management.

* Step 3: The network policy is delivered to relevant 5G Core functions and connected security components. These components then prepare for the enforcement of the policy.

* Step 4: The application policy is sent to the IBN Controllers on the target user devices. This allows the devices to receive instructions without direct user intervention.

* Step 5: Each device applies the policy to adjust its settings and behavior. The changes take effect locally to reflect the system-wide intent.

* Step 6: Devices monitor their own status and send relevant data back to their IBN Controllers. This ensures continuous awareness of policy impact at the device level.

* Step 7: IBN Controllers compile and forward the data as monitoring reports. These reports provide a basis for evaluating the effectiveness of the applied policies.

* Step 8: The reports are analyzed to check if the policies are working as intended, and the results are stored for future use. This completes the feedback loop that enables adaptive policy refinement.

Through this process, the system enables intent-driven security management that spans from core network functions to individual user devices. By translating high-level intents into enforceable policies and continuously monitoring their effects, the architecture supports real-time adaptation to network conditions and user behaviors. This ensures that security enforcement remains consistent, context-aware, and autonomous throughout distributed edge environments. Moreover, the closed-loop structure provides a foundation for scalable and self-optimizing policy management, which is essential for future 5G edge-native networks.

Also, the proposed system extends the core components such as the Intent-Based Networking Use Function (IUF), Intent Control Function (ICF), and distributed enforcement modules to operate in tandem with the handover procedures defined in 3GPP specifications. This helps keep security consistent and smart across the edge network where quick response and local control are especially important. This approach can also be applied to mobility scenarios where intent-driven security policies need to dynamically migrate and be re-enforced as User Equipment (UE) transitions between gNBs.

5. Security Considerations Sections

In the context of intent-based edge security management in 5G networks, several important security aspects must be considered to ensure robust and trustworthy system behavior. One key concern involves the potential for malicious manipulation of user intents. Since intents are high-level expressions of user goals that drive the automated generation of network and application policies, any unauthorized alteration could lead to unintended or insecure outcomes. Ensuring that each intent originates from a trusted source and is protected by integrity validation mechanisms is therefore essential.

Another important consideration is the accuracy and reliability of the policy translation and enforcement process. When translating abstract intents into concrete policies, the system must preserve the user’s original intent without introducing misconfigurations or inconsistencies. Incorporating validation checks and feedback mechanisms helps ensure that policies are correctly interpreted and consistently applied across the network. To further enhance this process, deep learning techniques [Deep-Learning] can be employed to detect anomalies, learn from past policy enforcement outcomes, and adaptively improve the translation logic based on contextual patterns and historical data.

6. IANA Considerations

This document does not require any IANA actions.

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>.

7.2. Informative References

[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.

[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-29.503] "Service-Based Interface Specifications for the Network Exposure Function (NEF)", Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3342, 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, December 2014.

[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.

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

[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.

[ClickINC-Sigcomm-2023]
Xu, W., Zhang, Z., Feng, Y., Song, H., Chen, Z., Wu, W., Liu, G., Zhang, Y., Liu, S., Tian, Z., and B. Liu, "ClickINC: In-network Computing as a Service in Heterogeneous Programmable Data-center Networks", Publisher: ACM SIGCOMM, Available: https://dl.acm.org/doi/10.1145/3603269.3604835, September 2023.

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 and RS-2022-II221015).

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. IITP-2025-RS-2022-II221199, Regional strategic industry convergence security core talent training business).

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
Email: rna0415@skku.edu
URI: http://iotlab.skku.edu/people-Moses-Gu.php

Authors' Addresses

Yoseop Ahn (editor)
Department of Computer Science & Engineering
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon
Gyeonggi-Do
16419
Republic of Korea
Phone: +82 31 299 4106
Email: ahnjs124@skku.edu
URI: http://iotlab.skku.edu/people-Ahn-Yoseop.php

Jaehoon Paul Jeong (editor)
Department of Computer Science & 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

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

Email: younghak@ssu.ac.kr