RADCOM NWDAF

5G analytics for closed-loop operations

RADCOM

The information, content or material herein is provided "AS IS", is designated confidential and is subject to all restrictions in any law regarding such matters, and the relevant confidentiality and non-disclosure clauses or agreements issued prior to and/or after the disclosure. All the information in this document is to be safeguarded and all steps must be taken to prevent it from being disclosed to any person or entity other than the direct entity that received it directly from RADCOM.

The text and drawings herein are for the purpose of illustration and reference only.

RADCOM reserves the right to periodically change information that is contained in this document; however, RADCOM makes no commitment to provide any such changes, updates, enhancements or other additions to this document to you in a timely manner or at all.

Publication Date: April 22

Website:
http://www.radcom.com

INTRODUCTION

RADCOM NWDAF is an open, standards-compliant, and vendor-agnostic solution that provides all the 3GPP use cases defined in Rel. 15, 16, and 17. Collecting and correlating data from multiple sources (subscription/notification events, event data records, packets, and fault management (FM) and performance management (PM) data). In addition, RADCOM's underlying solution architecture for the NWDAF can also be utilized as a RAN-DAF and MDAF.

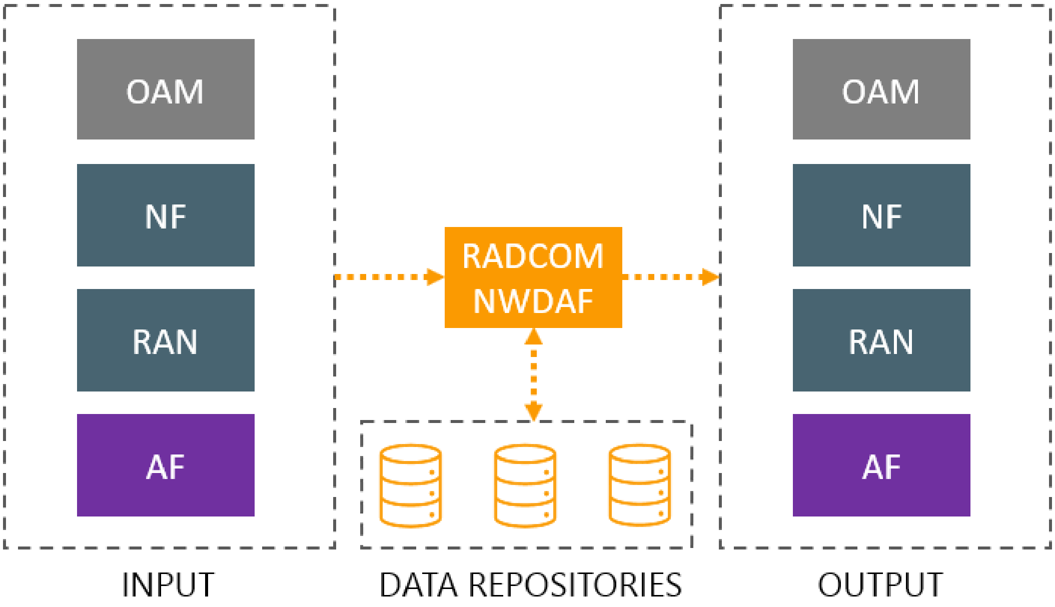


Figure 1 - RADCOM NWDAF provides a centralized data analytics function for 5G

RADCOM NWDAF leverages open, standardized interfaces to share data with the other network functions as a producer/consumer in the 5G core. While data is exposed with a REST API to the service layer, UI, and application layer, it can leverage standard services to scale, such as web load balancers, security services for HTTPS-based access, and more.

3GPP use cases

As part of Release 16 and 17, the following consumers of NWDAF data have been added (alongside the PCF and NSSF for network slicing in Release 15). The full list of consumers is:

- Access and Mobility Management Function (AMF)
- Application Function (AF)
- Network Exposure Function (NEF)
- Network Slice Selection Function (NSSF)
- Operation, Administration, and Maintenance (OAM)
- Policy Control Function (PCF)
- Session Management Function (SMF)
- Unified Data Management (UDM)

3GPP use cases for NWDAF in Releases 16 and 17:

- Dispersion analytics
- DN performance analytics
- Expected UE behavioral parameters related to network data analytics
- Network performance analytics
- NF load analytics
- Observed service experience related to network data analytics
- QoS sustainability analytics
- Redundant transmission experience related analytics
- Session management congestion control experience analytics
- Slice load level related network data analytics use case
- UE communication analytics
- UE mobility analytics
- User data congestion analytics
- WLAN performance analytics

In the upcoming Release 17 (expected to be completed in June 2022), the 3GPP specifies changes in the RADCOM NWDAF architecture:

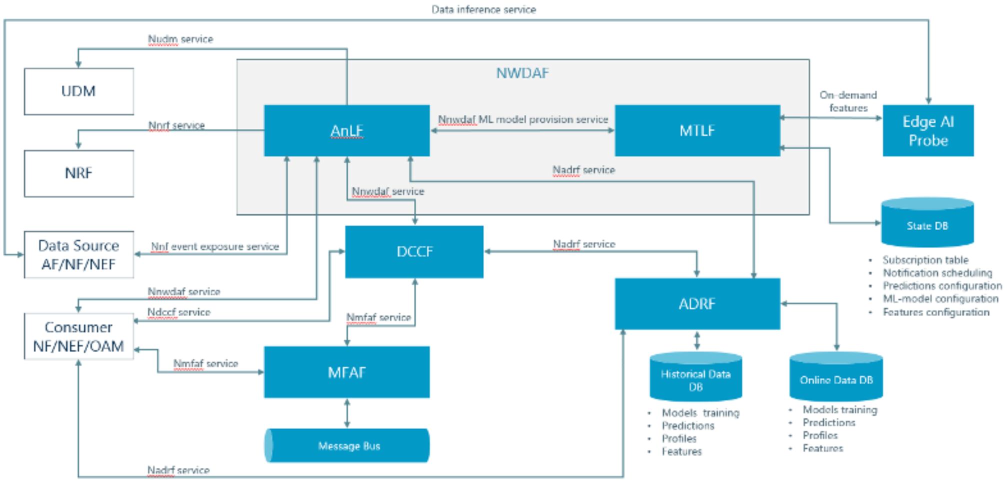


Figure 2 - NWDAF architecture in Rel.17

Introducing the following functions:

- Analytics Logical Function (AnLF)
- Model Training Logical Function (MTLF)
- Data Collection Coordination Function (DCCF)
- Analytics Data Repository Function (ADRF)
- Messaging Framework Adaptor Function (MFAF)

Extended use cases

In addition to 3GPP-defined use cases, RADCOM NWDAF can be extended above and beyond the standard use cases, frameworks, interfaces, and APIs. This includes collecting and correlating proprietary vendor event feeds and exporting data analytics through non-3GPP APIs. Enabling RADCOM to offer unique value to telecom operators, such as creating user plane KPIs/KQIs for insights into the real-life customer experience as well as additional use cases beyond the 3GPP specifications, examples include:

- O-RAN optimization (core KPIs are sent to the RAN Intelligent Controller)
- Signaling storm mitigation
- Automated disaster recovery
- Mass call event optimization
- IoT anomaly detection
- Unauthorized tethering and network hogs

Covering 3GPP standards and proprietary use cases, RADCOM NWDAF becomes the central analytics function with the 5G core, providing real-time network and subscriber insights to drive zero-touch, closed-loop network automation for all services.

RADCOM solution advantages:

Built-in Artificial Intelligence (AI)

Automation will play an essential part in unlocking the potential of 5G, and NWDAF will provide a critical role in helping operators make strides towards this goal and transition to zero-touch network management. This will mean the network adapts automatically to changing traffic conditions and demands without human intervention through this centralized analytics function, empowering operators with a closed-loop approach to network operations and service quality monitoring.

For example, using AI-driven insights for network slicing means that slices can be created dynamically with on-demand network resources. The service delivery policy is set to match the required QoS. The network slices will be monitored for performance and adjusted according to the resources necessary to deliver the agreed SLA. AI and ML will be continually utilized to assist zero-touch slice management by forecasting resource utilization trends and proactively improving/configuring the network resources.

Anomaly detection, RCA, and predictive analytics

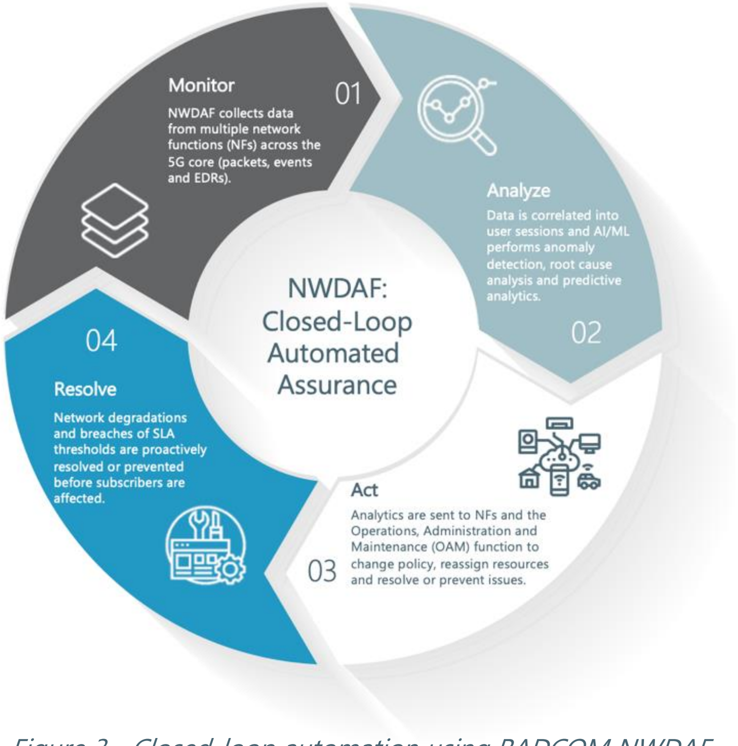
RADCOM NWDAF goes beyond the 3GPP-defined AI framework that focuses on predictive analytics. With RADCOM NWDAF powered by RADCOM AIM (AI module), the operator also benefits from additional Artificial Intelligence (AI) and Machine Learning (ML) driven use cases such as automated anomaly detection and root cause analysis.

RADCOM AIM provides this without any need to configure thresholds. So, once RADCOM's solution is deployed on the network, it learns baseline behavior and automatically creates thresholds. Then, if an anomaly is detected, a closed-loop task is activated by sending a notification to 3rd part network functions or the Operations, Administration, and Maintenance (OAM), which facilitates corrective action using a zero-touch process with no human interaction.

The centralized repository of data analytics combined with AI and ML will enable operators to manage their networks efficiently and assure that QoS requirements are met even when rapid changes in the network traffic occur. This type of automation will be critical with such services as mission-critical communications or other latency-sensitive services widely deployed on 5G.

Closed-loop automation

RADCOM NWDAF introduces a new level of intelligence to the 5G network by combining end-to-end analytics, AI, and its seamless integration into the Operations, Administration, and Management (OAM) function to automate network operations. This closed-loop automation will be essential for guaranteeing QoS and QoE while ensuring network performance, resource management, and operational savings. RADCOM NWDAF acts as the conductor that ensures that all services and network functions work in unison to deliver a quality experience to the subscriber. In addition, with auto-discovery functions built-in to RADCOM NWDAF, new network functions and services can be tested and monitored as they roll out.



NWDAF collects data from multiple network functions (NFs) across the 5G core (packets, events and EDRs).

Data is correlated into user sessions and AI/ML performs anomaly detection, root cause analysis and predictive analytics.

Analytics are sent to NFs and the Operations, Administration and Maintenance (OAM) function to change policy, reassign resources and resolve or prevent issues.

Network degradations and breaches of SLA thresholds are proactively resolved or prevented before subscribers are affected.

Figure 3 - Closed-loop automation using RADCOM NWDAF

Flexible NWDAF architecture

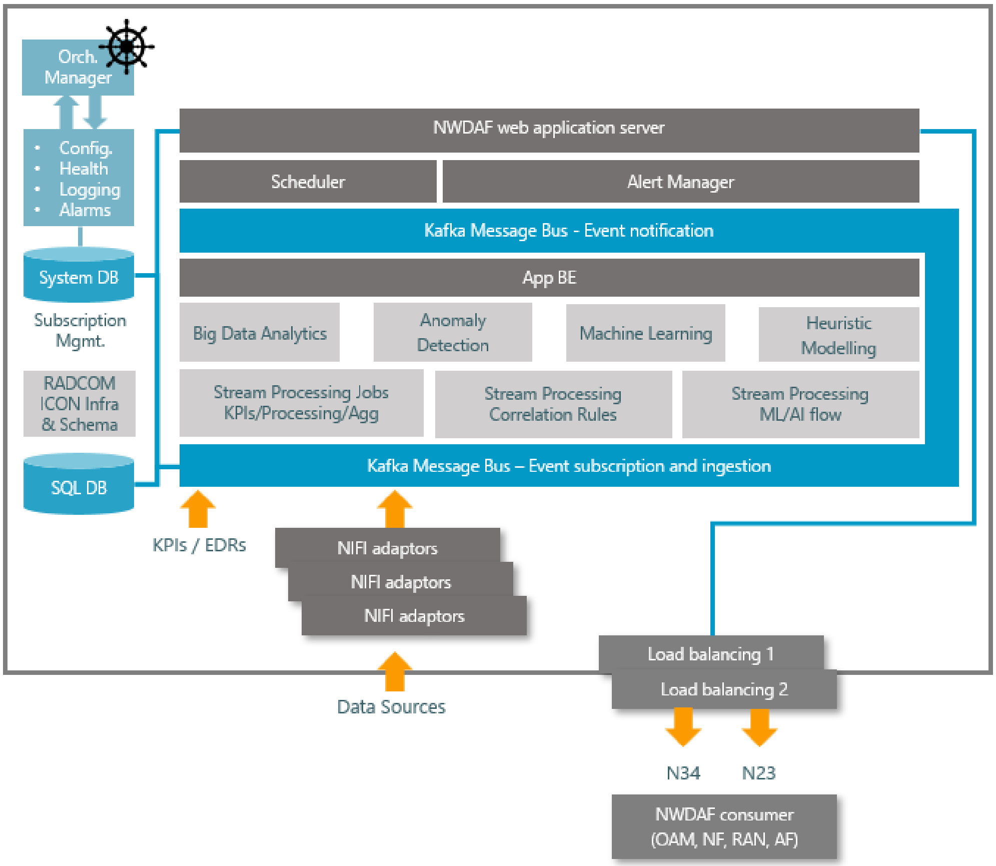

Orch. Manager
Config.
Health
Logging
Alarms
System DB
Subscription Mgmt.
RADCOM ICON Infra & Schema
SQL DB
NWDAF web application server
Scheduler
Alert Manager
Kafka Message Bus - Event notification
App BE
Big Data Analytics
Anomaly Detection
Machine Learning
Heuristic Modelling
Stream Processing Jobs KPIs/Processing/Agg
Stream Processing Correlation Rules
Stream Processing ML/AI flow
Kafka Message Bus – Event subscription and ingestion
KPIs / EDRs
NIFI adaptors
NIFI adaptors
NIFI adaptors
Data Sources
Load balancing 1
Load balancing 2
N34
N23
NWDAF consumer (OAM, NF, RAN, AF)

Figure 4 - RADCOM NWDAF architecture

RADCOM can provide the following NWDAF options to operators:

1. A 3GPP-defined NWDAF that includes standard APIs and network interfaces. This option covers all the use cases defined in Rel. 15, 16, and 17.
2. An extended NWDAF solution beyond the standards that includes closed-loop options, additional interfaces, and probe data ingestion. This option adds proprietary use cases in addition to the 3GPP-defined ones.
3. A lightweight “skinny” NWDAF deployment with a front-end NWDAF deployed in the 5G core. While the heavy lifting is performed outside the core via a centralized back-end.

NWDAF use cases

Use case	Description
Automated disaster recovery	By detecting anomalous network behavior related to a disaster event, a set of actions can be performed to ensure a stable service. A collection of priorities are determined to guide the correct resource allocation. It is constructed by service, geographical, and network function priorities. The leading guidelines are to secure minimum service levels for prioritized services and customers for a required time. Criteria such as average battery backup configurations for core and RAN, indoor/outdoor coverage requirements, voice-only services, and the number of emergency personnel deployed can all be considered. An automated process is performed to activate secondary sites in case of a complete outage at the primary site. A manual command can abort the disaster recovery state.
Customize mobility management	The NWDAF can mine the collected network information to precisely predict UE's mobility pattern and the associated UE track, e.g., gNB list or cell list per time of day. Then provide feedback on the gathered analytics, allowing the AMF to page the UE via, e.g., gNB list or cell list, bringing down the paging load in gNB and saving related processing resources in gNB.
Determining areas with fluctuating network conditions	By correlating and analyzing information from the network functions with data from the application functions (like MOS), RADCOM's NWDAF can provide statistical information that enables operators to change network deployment and configuration to improve E2E QoS. Examples of improvements that can be triggered are that RADCOM's NWDAF will correlate service data with data provided by the NFs to find out why the service experience is low. The AF can be informed when a UE is approaching a potentially overloaded area so that the AF can know that there is a higher chance of service fluctuation in these network conditions.

Use case	Description
Dispersion analytics	Dispersion analytics identifies the location (i.e., areas of interest, TAs, cells) or network slice(s) where a UE, or a group of UEs, or any UE disperse most (if not all) of their data volume and sessions transactions (i.e., MM and SM messages). The NWDAF collects UE dispersion-related information from the NFs and provides dispersion statistics and predictions.
DN performance analytics	The NWDAF provides analytics for user plane performance (i.e., average traffic rate, average packet delay) in the form of statistics or predictions to a service consumer.
Expected UE behavioral parameters related network data analytics	A service consumer learns from the NWDAF the expected UE behavior parameters as defined in TS 23.502 for a group of UEs or a specific UE. The service consumer can be an NF or the OAM.
Management of Massive IoT (MIoT) infrastructure	Service behaviors, data traffic (frequency, size), and locations probably have apparent regularity in some vertical industries. However, for MIoT, the use cases are diversified, and the behaviors of MIoT terminals may vary a lot for different use cases, so requirements for quality of service and power saving are different. By utilizing both the NWDAF and NSSF, the expected UE behavioral information can be sent to the UDM to help supervise MIoT terminals. The NWDAF can also help IoT anomaly detection (see the Signaling storm mitigation use case).
Mass call event optimization	During a mass call event (either planned or not planned), the network resources are challenged by (sometimes unpredictable) change demands. To avoid significant QoE degradation or a complete network function outage, a series of actions need to be taken and initiated by the NWDAF. The initial step is to detect an occurrence of a mass call event. At the same time, a continuous close monitoring cycle is performed to evaluate NF load and stability state. According to the NF state, as a mass call event develops, actions are taken to balance the network load and ensure network stability. As the mass call event conditions pass, NF settings are returned to the pre-event configuration.

Use case	Description
Network performance analytics	NWDAF provides either statistics or predictions on the gNB status information, gNB resource usage, communication performance, and mobility performance in an Area of Interest. In addition, the NWDAF provides statistics or predictions on the number of UEs in that Area of Interest. The service consumer may be an NF (e.g., PCF, NEF, AF) or the OAM.
NF load analytics	In the form of statistics or predictions, or both, load analytics are provided by the NWDAF to a service consumer (NF) or the OAM. If a list of the NF Instance IDs is provided, the NWDAF offers the analytics for each designated NF instance. Otherwise, if a SUPI is provided, the NWDAF shall use the SUPI to determine which NF instances (AMF and SMF) are serving this specific UE, filter them according to the provided S-NSSAI and NF types using data collected from NRF or OAM, and provide analytics for these NF instances.
Observed service experience related network data analytics	Provides Observed Service Experience (i.e., average of observed Service MoS and/or variance of observed Service MoS indicating service MOS distribution for services such as audio-visual streaming as well as services that are not audio-visual streaming such as V2X and Web Browsing services) analytics, in the form of statistics or predictions, to a service consumer. Analytics can cover the service experience for a network slice (for a UE or a group of UEs) and service experience in an application (or group of applications).
Optimization of network slicing	The NWDAF identifies each network slice by the Single Network Slice Selection Identifier (S-NSSAI), which includes the following components: • Slice/Service Type (SST) and optional • Slice Differentiator (SD) The PCF takes input from the NWDAF to assign more resources or steer traffic policies, while the NSSF takes the load level information for slice selection. User plane and control plane transactions are associated with the SST, and SD and KPIs are aggregated by the SST and SD (exposed via the 3GPP standard interfaces). With built-in, AI/ML capabilities can provide a closed-loop solution that analyzes network data, sets thresholds, and automatically detects anomalies with no human input required. This enables operators to roll out multiple slices and monitor/maintain SLAs automatically without manual configuration.

Use case	Description
QoS sustainability analytics	The consumer of QoS Sustainability analytics can request analytics regarding the QoS change statistics for the analytics target period in a specific area or the likelihood of a QoS change for the analytics target period in the future in a particular site. The consumer (an NF, e.g., AF) can request to subscribe to notifications or a single message.
RAN optimization	The NWDAF enriches the non-RT RAN Intelligent Controller (RIC) with core KPIs, which helps improve network optimization decisions.
Redundant transmission experience related analytics	This type of analytics provided by the NWDAF can be used by the SMF to determine whether redundant transmission shall be performed or if it had been activated to stop.
Session management congestion control experience analytics	The SMF service consumer can request the NWDAF to provide Session Management Congestion Control Experience (SMCCE) statistical analytics for a specific DNN and S-NSSAI. The SMF uses the potential congestion condition as a trigger to request the SMCCE analytics from the NWDAF.
Signaling storm mitigation	The NWDAF can help detect security-related anomalies. For example, if many IoT devices become infected with malware, they can create IoT clusters that could create a massive signaling storm. This type of bandwidth consumption anomaly is something that NWDAF can detect. When an IoT device produces a few megabytes of data and then starts to produce gigabytes per hour, that needs attention. The NWDAF provides these analytics to an NF or OAM
Slice load level related network data analytics use case	NWDAF provides slice load level information to an NF on a Network Slice instance level. The NWDAF notifies slice-specific network status information to the NFs that are subscribed to it. An NF may collect directly slice specific network status information from the NWDAF. This information is not subscriber specific.
UE communication analytics	To support some optimization operations, e.g., customized mobility management, traffic routing handling, or QoS improvement, the NWDAF can perform data analytics on UE communication patterns and user plane traffic and provide the analytics results (i.e., UE communication statistics or prediction) to the NFs. The NWDAF collects per-application communication descriptions from AFs. If the consumer NF provides an Application ID in the request to the NWDAF, the NWDAF only considers data from the AF, SMF, and UPF that corresponds to this application ID.
UE mobility analytics	The NWDAF collects UE mobility-related information from the NF, OAM and provides statistics or predictions to the consumer (an NF, e.g., AMF).

Use case	Description
Unauthorized tethering and network hogs	The NWDAF provides insights about the devices connected to the network and can provide unauthorized tethering and network hog data. Device analytics that the NWDAF can offer are volume, type, and frequency of network traffic on both IoT devices and smartphones. The NWDAF then calculates a statistical baseline to compare device traffic patterns to identify the fraudulent use of network resources. NWDAF uses AI/ML algorithms to detect UEs that perform unauthorized or abusive tethering and triggers required action according to the Service Provider's definitions, e.g., Send a warning SMS to the UE, limit the quota of UE or bar the UE. The NWDAF can initiate policies to limit network use for bandwidth hogs, such as restricting downlink bandwidth, limiting uplink bandwidth, reducing QoS, blocking data services, etc.
User data congestion analytics	The NWDAF provides user data congestion analytics by one-time reporting or continuous reporting, in the form of statistics or predictions, to another NF. The analytics can relate to the congestion experienced while transferring user data over the control plane or user plane, or both. The analytics can relate to a specific area or a particular user. Suppose the consumer of these analytics provides a UE ID. In that case, the NWDAF determines the area where the UE is located and collects measurements per cell, and uses the measurements to determine user data congestion.
WLAN performance analytics	Analytics are generated based on the data from other NFs and OAM and provide statistics or predictions containing the quality and performance of the WLAN connection of the UE according to UE location and SSID.

Additional use cases

Use case	Description
5G edge computing	The NWDAF is used to aid in SMF routing decisions
Access Traffic Steering, Switching, and Splitting (ATSSS) schemes support	The output of the NWDAF will feed new network functions related to Access Traffic Steering, Switching, and Splitting schemes (ATSSS). The three primary operations supported by the ATSSS are: • Access Traffic Steering: selects an access network for new data flow and transfers the traffic of this data flow over the access network chosen • Access Traffic Switching: The procedure that moves all traffic of ongoing data flow from one access network to another in a way that maintains the continuity of the data flow • Access Traffic Splitting: The procedure that splits data flow traffic across multiple access networks. When traffic splitting is applied to a data flow, some traffic of the data flow is transferred via one access, and some other traffic of the same data flow is transferred via another access system
Prevention of security attacks/anti-fraud	The NWDAF is used with real-time machine learning to execute fraud prediction and prevent security attacks on the network. This is done by calculating a statistical baseline to compare device traffic patterns to identify the fraudulent use of network resources.