Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 13 November 2025

B. Sarikaya
Unaffiliated
R. Schott
Deutsche Telekom

12 May 2025

Security and Privacy Implications of 3GPP AI/ML Services for 6G
draft-sarischo-6gip-aiml-security-privacy-05

Abstract

This document provides an overview of 3GPP work on Artificial Intelligence/ Machine Learning (AI/ML) services. Application areas and corresponding proposed modifications to the architecture are identified. Security and privacy issues of these new applications need to be identified out of which IETF work could emerge.

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 13 November 2025.

Copyright Notice

Table of Contents

1. Introduction 2
2. Training and Federated Learning 4
3. Architecture 5
3.1. AI/ML for Vertical Markets 7
4. AI/ML in Radio Access Network 7
4.1. AI/ML in Open Radio Access Network 8
5. Security and Privacy 8
6. Work Points 10
7. Transfer Learning Use Case 11
8. Future Work 12
9. Security Considerations 12
10. IANA Considerations 12
11. Acknowledgements 12
12. References 12
12.1. Normative References 12
12.2. Informative References 13
Authors' Addresses 15

1. Introduction

Artificial Intelligence (AI) has historically been defined as the science and engineering to build intelligent machines capable of carrying out tasks as humans do. Inspired from the way human brain works, machine learning (ML) is defined as the field of study that gives computers the ability to learn without being explicitly programmed. Since it is believed that the main computational elements in a human brain are 86 billion neurons, the more popular ML approaches are using "neural network" as the model. Neural networks (NN) take their inspiration from the notion that a neuron's computation involves a weighted sum of the input values. A computational neural network contains the neurons in the input layer which receive some values and propagate them to the neurons in the middle layer of the network, which is also called a "hidden layer". The weighted sums from one or more hidden layers are ultimately propagated to the output layer, which presents the final outputs of the network.

Neural networks having more than three layers, i.e., more than one hidden layer are called deep neural networks (DNN). In contrast to the conventional shallow-structured NN architectures, DNNs, also referred to as deep learning, made amazing breakthroughs since 2010s in many essential application areas because they can achieve human-level accuracy or even exceed human accuracy. Deep learning techniques use supervised and/or unsupervised strategies to automatically learn hierarchical representations in deep architectures for classification. With a large number of hidden

layers, the superior performance of DNNs comes from its ability to extract high-level features from raw sensory data after using statistical learning over a large amount of data to obtain an effective representation of an input space. In recent years, thanks to the big data obtained from the real world, the rapidly increased computation capacity and continuously-evolved algorithms, DNNs have become the most popular ML models for many AI applications.

The performance of DNNs is gained at the cost of high computational complexity. Hence more efficient compute engines are often used, e.g. graphics processing units (GPU) and network processing units (NPU). Compared to the inference which only involves the feedforward process, the training often requires more computation and storage resources because it involves also the back propagation process.

Many DNN models have been developed over the past two decades. Each of these models has a different "network architecture" in terms of number of layers, layer types, layer shapes (i.e., filter size, number of channels and filters), and connections between layers. Three popular structures of DNNs: multilayer perceptron (MLPs), convolution neural networks (CNNs), and recurrent neural networks (RNNs). Multilayer perceptron (MLP) model is the most basic DNN, which is composed of a series of fully connected layers. In a fully connected layer, all outputs are connected to all inputs. Hence MLP requires a significant amount of storage and computation.

A convolution neural network (CNN) is composed of multiple convolutional layers. Applying various convolutional filters, CNN models can capture the high-level representation of the input data, making it popular for image classification and speech recognition tasks.

Recurrent neural network (RNN) models are another type of DNNs, which use sequential data feeding. The input of RNN consists of the current input and the previous samples. RNN models have been widely used in the natural language processing task on mobile devices, e.g., language modeling, machine translation, question answering, word embedding, and document classification. RNN models and their derivative Large Language Model (LLM) are out of scope.

While AI/ML has very many applications, in this document, we are interested in it AI/ML based services in mobile networks [MaTeMaFiWeKo21]. One is the network optimization comprises of the time-series forecasting, predictive maintenance, Quality of Experience (QoE) modeling and the other is speech recognition, image recognition, video processing all of them characterized as network analytics. When network analytics is used in the mobile network, the end device is the base station. For the speech/ image recognition

and video processing (mainly used in the vertical markets such as autonomous cars, smart factories) the end device is the UE [TR22.874].

AI/ML has other applications as well in improving radio access network (RAN). DNN models can be used for the New Radio (NR) air interface. Use cases are channel state information (CSI) feedback enhancement, beam management, and positioning accuracy enhancements [Lin23] and [Lin24].

This document aims to present issues of Artificial Intelligence Machine Learning (AIML) based services in mobile networks that may require further protocol work, mostly on the security and privacy aspects. It is expected that the next generation 6G air interface will emerge from AI/ML applications to the NR air interface, and network operation will benefit from the network analytics enhancements offered by AI/ML.

2. Training and Federated Learning

Training is a process in which an AI/ML model learns to perform its given tasks, more specifically, by optimizing the value of the weights in the DNN. A DNN is trained by inputting a training set, which are often correctly-labelled training samples. Taking image classification for instance, the training set includes correctly-classified images. The training process is repeated iteratively to continuously reduce the overall loss. Until the loss is below a predefined threshold, the DNN with high precision is obtained. After a DNN is trained, it can perform its task by computing the output of the network using the weights determined during the training process, which is referred to as inference. In the model inference process, the inputs from the real world are passed through the DNN. Then the prediction for the task is output. For instance, the inputs can be pixels of an image, sampled amplitudes of an audio wave or the numerical representation of the state of some system or game. Correspondingly, the outputs of the network can be a probability that an image contains a particular object.

With continuously improving capability of cameras and sensors on mobile devices, valuable training data, which are essential for AI/ML model training, are increasingly generated on the devices. For many AI/ML tasks, the fragmented data collected by mobile devices are essential for training a global model. In the traditional approaches, the training data gathered by mobile devices are centralized to the cloud datacenter for a centralized training.

In Distributed Learning mode, each computing node trains its own DNN model locally with local data, which preserves private information locally. To obtain the global DNN model by sharing local training improvement, nodes in the network will communicate with each other to exchange the local model updates. In this mode, the global DNN model can be trained without the intervention of the cloud datacenter.

In 3GPP Federated Learning (FL) mode, the cloud server trains a global model by aggregating local models partially-trained by each end devices. The most agreeable Federated Learning algorithm so far is based on the iterative model averaging whereby within each training iteration, a UE performs the training based on the model downloaded from the AI server using the local training data. Then the UE reports the interim training results (e.g., gradients for the DNN) to the cloud server via the uplink (UL) channels. The server aggregates the gradients from the UEs, and updates the global model. Next, the updated global model is distributed to the UEs via the Data Link (DL) channels. Then the UEs can perform the training for the next iteration.

Summarizing, we can say that distributed learning is about having centralized data but distributing the model training to different nodes, while Federated Learning (FL) is about having decentralized data and training and in effect having a central model [Srini21]

3. Architecture

A new framework for protocols called Service based architecture (SBA) comprises Network Functions (NFs) that expose services through RESTful Application Programming Interface (APIs) has been defined. There are providers and consumers (publishers and subscribers) which are new functions in the system [IsNo20]. SBA provides built in security using Public Key Infrastructure (PKI) managed certificates in the mobile core network.

For AI/ML, 3GPP core, aka mobile core network, has a new server function: The Network Data Analytics Function (NWDAF) provides analytics to Mobile Core Network Functions (NFs) and Operations and Management (OAM). An NWDAF may contain the Analytics logical function (AnLF): A logical function in NWDAF, which performs inference, derives analytics information and Model Training logical function (MTLF) which trains Machine Learning (ML) models and exposes new training services. The Application AI/ML operation logic is controlled by an Application Function (AF). Any AF request to the mobile network (which consists of the Mobile Core Network, access network and UE) in the context of the Mobile Core Network assistance to Application AI/ML operation should be authorized by the Mobile Core Network [TR23.700-80].

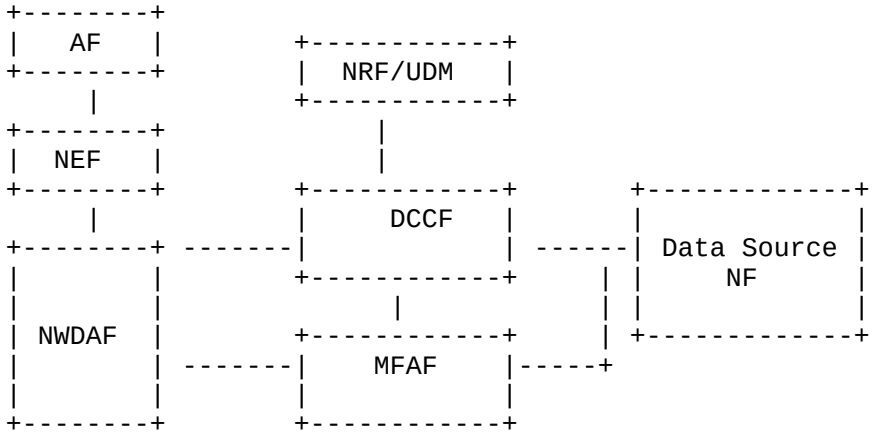

Figure 1: NWDAF and related components

NWDAF relies on various sources of data input including data from the mobile core NFs, AFs, e.g., Network Repository Function (NRF), Unified Data Management (UDM), etc., and OAM data, including performance measurements (PMs), Key Performance Indicators (KPIs), configuration management data and alarms. An NWDAF may provide in turn analytics output results to the mobile core NF, AFs, and OAM. Optionally, Data Collection Coordination Function (DCCF) and Messaging Framework Adaptor Function (MFAF) may be involved to distribute and collect repeated data towards or from various data sources. Note that AF contains a Network Exposure Function (NEF) if it is an untrusted AF, i.e. external to the operator's network. NEF may assist the AI/ML application server in scheduling available UE(s) to participate in the AI/ML operation, e.g., Federated Learning Figure 1 [TS23.288]. Also, Mobile Core Network may assist the selection of UEs to serve as FL clients, by providing a list of target member UE(s), then subscribing to NWDAF via the NEF to be notified about the subset list of UE(s) (i.e., list of candidate UE(s)) that fulfill certain filtering criteria (not shown in the figure) [TR23.700-82].

In Next Generation Radio Access Network (NG-RAN), AI/ML support requires inputs from neighboring NG-RAN nodes and UEs. No special new node is added to the architecture for training and inference. AI/ML model training can be located in the OAM and model inference in the NG-RAN node or UE. It is also possible that both model training and inference are located in the NG-RAN node [TS38.300].

3.1. AI/ML for Vertical Markets

Vertical markets cover automotive such as cars, drones and IoT based smart factories are the major consumers of 3GPP-provided data analytics services [TS22.261]. They play important role on the Exposure of data analytics services from different network domains to the verticals in a unified manner. They define, at an overarching layer, value-add application data analytics services which cover stats/predictions for the end-to-end application service.

In order to allow the vertical market industries running applications over the mobile network a service enabler architecture which specifies the procedures, information flows and APIs called Application Data Analytics Enablement Service Enabler Architecture Layer (SEAL) for Verticals is defined [TS23.436]. SEAL applications can be hosted on the Edge of the mobile network for UE use at the Edge.

Example use case is the Vertical user leveraging the Application layer Analytics capabilities for predicting end to end performance and selecting the optimal Vertical Application Layer (VAL) server [TS23.436]. VAL uses the SEAL layer to realize its services.

[TR23.700-82] expands upon the data analytics as a useful tool to optimize the service offering by predicting events related to the network or UE conditions. These services however can also assist the 3rd party AI/ML application service provider for the AI/ML model distribution, transfer, training for various applications (e.g., video/speech recognition, robot control, automotive). This takes us to the concept of the application enablement layer can play role on the exposure of AI/ML services from different 3GPP domains to the Application Service Providers (ASP) in a unified manner.

4. AI/ML in Radio Access Network

AI/ML for New Radio (NR) Air Interface has these use cases: Channel State Information (CSI) feedback enhancement which involves overhead reduction, improved accuracy, prediction; beam management, and positioning accuracy enhancements [TR38.843].

For CSI, time domain CSI prediction employing one sided (usually at the UE) model training done by the vendor and inference done at the UE. This technique avoids CSI compression using two-sided AI/ML models where Deep Neural Network models are used by UE to encode, to compress CSI feedback information and a corresponding CSI decoder is used at the gNB to reconstruct the CSI from the received feedback data.

AI/ML is also used in beam management to support downlink beam forming with one sided (UE or gNB) models and positioning accuracy enhancements with direct UE side AI/ML positioning or UE-assisted or gNB-assisted LMF-based positioning.

Protocol mechanism is called data collection. It is for the purpose of AI/ML model training, data analytics and inference by the network nodes, management entity or UE. Xn Application Protocol over Xn interface defines a set of Data Collection messages used by an NG-RAN node 1 to request from another NG-RAN node 2 the reporting of information to support AI/ML in NG-RAN [TR38.423]. UE data collection is done by gNB requested by OAM and reported to the Access and Mobility management Function (AMF).

Radio Access Network AI/ML operations are based on Data Collection protocol procedures which are used in model training and model inference operations. Data Collection set of link layer messages are part of Xn Application Protocol defined in [TR38.423]. Stream Control Transmission Protocol (SCTP) is used to securely transport data collection messages in the Radio Access Network [RFC9260].

4.1. AI/ML in Open Radio Access Network

Open Radio Access Network (Open RAN) is a new approach to building RANs [WakaSB24]. Open RAN is about disaggregated RAN functionality built using open interface specifications between elements designed to support equipment interoperability from multiple vendors. In Open RAN, a base station is split into several functional components, including central unit (CU), distributed unit (DU), and a remote unit (RU). Open RAN introduces advanced automation into the RAN system by means of an abstracted entity to manage the radio networks, i.e. RAN Intelligent Controller (RIC).

RIC will contain specialized AI hardware needed to implement the execution of the models for CSI feedback enhancement, beam management and positioning accuracy enhancements discussed above.

5. Security and Privacy

AI/ML based aservices in mobile networks raise many security and privacy issues. [TR23.700-80] and [TR23.700-82] identify a number of key issues and [TR33.898] presents a study on one of the key issues which will be detailed here.

[TR23.700-80] studies the exposure of different types of assistance information such as traffic rate, packet delay, packet loss rate, network condition changes, candidate federated learning (FL) members, geographical distribution information, etc., to AF for AI / ML

operations. Some of assistance information could be user privacy sensitive, such as candidate FL members, geographical distribution, i.e. location information. There is a need to study how to protect such privacy-related assistance information. In addition, Mobile Core Network needs to determine which assistance information is required by AF to complete AI/ML operation and to avoid exposing information that is unnecessary for AI/ML operations.

Because of the use of Restful API which depend on the use of HTTP protocol, OAuth 2.0 [RFC6749] protocol seems to be the natural choice here for authorization.

One solution can be developed reusing existing mechanism for authorization of Mobile Core Network assistance information exposure to AF. The solution is based on reusing the OAuth 2.0-based authorization mechanism. OAuth 2.0 [RFC6749] protocol extends traditional client-server authentication by providing a third-party client with a token. Since such token resembles a different set of credentials compared to those of the resource owner, the device needs not be allowed to use the resource owner’s credentials to access protected resources.

UE privacy profile/local policies stored in a database can also be employed to authorize UE-related Mobile Core Network assistance information exposure. UE privacy profile/local policies may also contain protection policies that indicate how Mobile Core Network assistance information should be protected (e.g., using security techniques like encryption, integrity protection, etc.). NWDAF via Network Exposure Function (NEF) sends the UE-related Mobile Core Network assistance information to AF when the local policies/UE privacy profile allows authorizing the AF to access the information (see Figure 1). According to the local policies/UE privacy profiles, NWDAF may need to protect the Mobile Core Network assistance information with security mechanisms.

A common Application Programming Interface (API) Framework for the Mobile Core Network and
northbound APIs (called CAPIF) is defined to securely expose capabilities and events to 3rd party Application Functions, i.e. external (AF) via Network Exposure Function (NEF). The interface between the NEF and the Application Function needs integrity protection, replay protection, confidentiality protection for communication between the NEF and Application Function, and mutual authentication between the NEF and Application Function and protect internal Mobile Core network information. The NEF also enable secure provision of information in the 3GPP network by authenticated and authorized AFs.

Security should be provided to support the protection of user privacy sensitive assistance information being exposed to AF. TLS 1.3 [RFC8446] is used to provide integrity protection, replay protection and confidentiality protection for the interface between the NEF and the AF [TS33.501].

As for Radio Access Network AI/ML services use cases like CSI, beam management, position accuracy enhancement, UE uses NR-Uu interface to communicate with NG-RAN node using RRC protocol to send L3 cell/beam measurements, location, sensor and timing information. Radio Resource Control (RRC) messages communicated over the air interface causes security issues because they are not protected. Transport layer protocol SCTP is used only when two NG-RAN nodes are connected over Xn. In this case SCTP should be run below DTLS 1.3 [RFC9147] to provide communications privacy, prevent eavesdropping and detect tampering or message forgery [dtlssctp].

Any location/positioning information sent directly from UE to NG-RAN node causes privacy concern without user consent. Location information may be sent in RRC IDLE/INACTIVE state and also in CONNECTED state after the connection is established [TR38.843]. Location information received by NG-RAN node is sent to Location Management Function (LMF) in the mobile core network.

6. Work Points

Security and privacy of AI/ML based services and applications in mobile networks need further work. [TR33.898] provides solutions to only one of many possible key issues. Each key issue has been in depth investigated in [TR23.700-80] and [TR23.700-82] from which new solutions can be developed.

We list below only some of the key issues identified:

* Enhance the mobile core network to expose information to the UE to facilitate the operation of AI/ML applications (e.g., Model Training, Splitting and inference feedback etc.)

* Expose UE-related information to an AF ensuring that privacy and security requirements are met.

* Additional parameters to be provisioned to the mobile core network by an external party for the assistance to the operation of AI/ML applications.

* Whether and how the existing mobile core network data transfer/ traffic routing mechanisms are re-used or enhanced to support the transmission of the Application AI/ML traffic(s) between AI/ML endpoints (i.e., UE and AF)

* Information to be provided by the mobile core network to the AF can help the AF to select and manage the group of UEs which will be part of FL operation.

* Enhance the architecture and related functions to support application layer AI/ML services

* Support Federated Learning at application enablement layers

* Enhance the architecture and related functions to support management and/or configuration for split AI/ML operation, and in-time transfer of AI/ML models. The management and configuration aspects including discovery of required nodes for split AI/ML operation and support of different models of AI/ML operation splitting in which the AI/ML operation/model is split, e.g. for performing inference, into multiple parts according to the current task and environment.

* Support transfer learning at application enablement layers

The last key issue will be elaborated in the next section below.

7. Transfer Learning Use Case

Transfer Learning (TL) is the training of a machine learning (ML) technique where a model pre-trained on one task is fine-tuned for a new but related task. Transfer learning assumes a baseline model is already available in a repository in the mobile network provided by the source domain can be fine-tuned to quickly perform the same or similar tasks in the target domain with lesser amount of training data.

TL support involves many entities in the mobile network. ML models need to be stored in the repository entities. When storing, some information elements need to be added to the model, such as identity of the model consumer that is initiating the request, i.e. model consumer id. For transfer learning, Base Model ID could be added.

Transfer Learning solution should aim to provide support for Transfer Learning (TL) by discovering and selecting the base models to be used for similar tasks as pre-trained models. It involves first discovering repositories of pre-trained models in a given service area and then sending request messages to the repositories and collecting responses.

Security and privacy issues in all the messaging need to be investigated.

8. Future Work

A use case document is needed. We have listed the identified use cases and elaborated one of them above in this document. New set of use cases on Rule Based Automation, Autonomous Networks, Automated Testing, Energy Efficiency and so on could be added to the existing use cases. All or some of these usage areas of AI/ML can further be elaborated in a use case document. These use cases should make it clear why the security and privacy protocols are needed.

A problem statement on AI/ML based services in mobile networks document is needed. Such a document should identify the problems that possibly need a new protocol to be developed or need to identify extensions to an existing protocol. One possibility in that direction could be refining the work points identified above and formulating them in terms of existing or to be defined in the future security and privacy protocols.

A document describing security threat model on which AI/ML security and privacy enhancements can be developed [RFC6819].

9. Security Considerations

Security considerations of AI/ML services is TBD.

10. IANA Considerations

There are no IANA considerations for this document.

11. Acknowledgements

We acknowledge useful comments from Hesham ElBakoury, Marie-Jose Monpetit, Natalie Romo-Moreno that have led to many improvements in the document.

12. References

12.1. Normative References

[RFC6749] Hardt, D., Ed., "The OAuth 2.0 Authorization Framework", RFC 6749, DOI 10.17487/RFC6749, October 2012, <https://www.rfc-editor.org/rfc/rfc6749>.

[RFC6819] Lodderstedt, T., Ed., McGloin, M., and P. Hunt, "OAuth 2.0 Threat Model and Security Considerations", RFC 6819, DOI 10.17487/RFC6819, January 2013, <https://www.rfc-editor.org/rfc/rfc6819>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/rfc/rfc8446>.

[RFC9147] Rescorla, E., Tschofenig, H., and N. Modadugu, "The Datagram Transport Layer Security (DTLS) Protocol Version 1.3", RFC 9147, DOI 10.17487/RFC9147, April 2022, <https://www.rfc-editor.org/rfc/rfc9147>.

[RFC9260] Stewart, R., Txen, M., and K. Nielsen, "Stream Control Transmission Protocol", RFC 9260, DOI 10.17487/RFC9260, June 2022, <https://www.rfc-editor.org/rfc/rfc9260>.

12.2. Informative References

[dtlssctp] Txen, M., Tschofenig, H., and T. Reddy.K, "Datagram Transport Layer Security (DTLS) 1.3 for Stream Control Transmission Protocol (SCTP)", Work in Progress, Internet-Draft, draft-tuexen-tsvwg-rfc6083-bis-06, 21 October 2024, <https://datatracker.ietf.org/doc/html/draft-tuexen-tsvwg-rfc6083-bis-06>.

[IsNo20] Isaksson, M. and C. Norrman, "Secure Federated Learning in 5G Mobile Networks", December 2020, <https://www.ericsson.com/48df60/assets/local/reports-papers/research-papers/secure-federated-learning-in-5g-mobile-networks.pdf>.

[Lin23] Lin, X., "5G-Advanced evolution in 3GPP Release 19", December 2023, <https://arxiv.org/pdf/2312.15174>.

[Lin24] Lin, X., "Enhancing Next-Generation Connectivity", March 2024, <https://www.comsoc.org/publications/ctn/overview-ai-3gpps-ran-release-18-enhancing-next-generation-connectivity>.

[MaTeMaFiWeKo21] Manocha, J., "Accelerating the adoption of AI in programmable 5G networks", July 2021,

<https://www.ericsson.com/en/reports-and-papers/white-papers/accelerating-the-adoption-of-ai-in-programmable-5g-networks>.

[Srini21] Srinivasan, A., "Difference between distributed learning versus Federated Learning algorithms", November 2021, <https://www.kdnuggets.com/2021/11/difference-distributed-learning-federated-learning-algorithms.html>.

[TR22.874] 3rd Generation Partnership Project, "Study on traffic characteristics and performance requirements for AI/ML model transfer in 5GS", December 2021.

[TR23.700-80] 3rd Generation Partnership Project, "Study on 5G System Support for AI/ML-based Services", December 2022, <https://www.3gpp.org/ftp/Specs/archive/23_series/23.700-80/>.

[TR23.700-82] 3rd Generation Partnership Project, "Study on application layer support for AI/ML services", September 2024, <https://www.3gpp.org/ftp/Specs/archive/23_series/23.700-82/23700-82-j10.zip>.

[TR33.898] 3rd Generation Partnership Project, "Study on security and privacy of Artificial Intelligence/Machine Learning (AI/ML)-based services and applications in 5G", July 2023, <https://www.3gpp.org/ftp/Specs/archive/33_series/33.898/33898-i01.zip>.

[TR38.423] 3rd Generation Partnership Project, "NG-RAN; Xn application protocol (XnAP)", December 2024, <https://www.3gpp.org/ftp/Specs/archive/38_series/38.423/38423-i40.zip>.

[TR38.843] 3rd Generation Partnership Project, "Study on Artificial Intelligence (AI)/Machine Learning (ML) for NR air interface", January 2024, <https://www.3gpp.org/ftp/Specs/archive/38_series/38.843/38843-i00.zip>.

[TS22.261] 3rd Generation Partnership Project, "Service Requirements for the 5G System", December 2024.

[TS23.288] 3rd Generation Partnership Project, "Architecture enhancements for 5G System (5GS) to support network data analytics services", December 2024, <https://www.3gpp.org/ftp/Specs/archive/23_series/23.288/23288-j10.zip>.

[TS23.436] 3rd Generation Partnership Project, "Functional architecture and information flows for Application Data Analytics Enablement Service", September 2024, <https://www.3gpp.org/ftp/Specs/archive/23_series/23.436/23436-j20.zip>.

[TS33.501] 3rd Generation Partnership Project, "Security Architecture and Procedures for 5G System", January 2025, <https://www.3gpp.org/ftp/Specs/archive/33_series/33.501/33501-j10.zip>.

[TS38.300] 3rd Generation Partnership Project, "Radio Access Network; NR; NR and NG-RAN Overall Description", December 2024, <https://www.3gpp.org/ftp/Specs/archive/38_series/38.300/38300-i40.zip>.

[WakaSB24] Wakikawa, R., "AI-RAN Telecom Infrastructure for the Age of AI", December 2024, <https://www.softbank.jp/corp/set/data/technology/research/story-event/Whitepaper_Download_Location/pdf/SoftBank_AI_RAN_Whitepaper_December2024.pdf>.

Authors' Addresses

Behcet Sarikaya
Unaffiliated
Email: sarikaya@ieee.org

Roland Schott
Deutsche Telekom
Deutsche-Telekom-Allee 9
64295 Darmstadt
Germany
Email: Roland.Schott@telekom.de