**3GPP TSG-SA5 Meeting #143eS5-223396**

**09 - 17 May 2022, E-meeting**

**Source: Nokia**

**Title: pCR 28.105 Add requirements for Sandboxing AI/ML**

**Document for: Approval**

**Agenda Item: 6.6.5**

# 1 Decision/action requested

***The group is asked to discuss and agree on the proposal.***

# 2 References

[1] 3GPP TS 28.105-100 “Management and orchestration; AI/ML management”.

# 3 Rationale

The AI/ML execution needs to be sandboxed to confirm its appropriateness before deployment in a production environment. This pCR presents the corresponding requirements.

# 4 Detailed proposal

|  |
| --- |
| **Start of modifications** |

# 4 Concepts and overview

## 4.1 Overview

The AI/ML techniques and relevant applications are being increasingly adopted by the wider industries and proved to be successful. These are now being applied to telecommunication industry including mobile networks.

Although AI/ML techniques in general are quite mature nowadays, some of the relevant aspects of the technology are still evolving with some new techniques are frequently emerging.

The AI/ML techniques can be generally characterized from different perspectives including the followings:

- **Learning methods**

The learning methods include supervised learning, unsupervised learning and reinforcement learning. Each learning method is fit to one or more specific category of inference (e.g., prediction), and requires specific type of training data. A brief comparison of these learning methods is provided in table 4.2-1.

Table 4.2-1: Comparison of Learning methods

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Supervised learning | Semi-supervised learning | **Unsupervised learning** | **Reinforcement learning** |
| Category of inference | Regression (numeric), classification | Regression (numeric), classification | Association, Clustering | Reward-based behaviour |
| Type of training data | Labelled data (Note 1) | Labelled data (Note 1), and unlabelled data | Unlabelled data | Not pre-defined |
| NOTE 1: The labelled data means the input and output parameters are explicitly labelled for each training data example. | | | | |

- **Learning complexity**

As per the learning complexity, there are Machine Learning (basic) and Deep Learning.

- **Learning architecture**

Based on the location where the learning takes place, the AI/ML can be categorized to centralized learning, distributed learning and federated learning.

- **Learning continuity**

From learning continuity perspective, the AI/ML can be offline learning or continuallearning.

Artificial Intelligence / Machine Learning (AI/ML) capabilities are used in various domains in 5GS, including management and orchestration (e.g., MDA, see TS 28.104 [2]) and 5G networks (e.g., NWDAF, see 23.288 [3]).

The AI/ML-enabled function in the 5GS uses the AI/ML model for inference.

Each AI/ML technique, depending on the adopted specific characteristics as mentioned above, may be suitable for supporting certain type/category of use cases in 5GS.

To enable and facilitate the AI/ML capabilities with the suitable AI/ML techniques in 5GS, the AI/ML model and AI/ML-enabled function (i.e., inference function) need to be managed. The term AI/ML Entity shall be used to refer to any entity that is either an AI/ML Model or contains an AI/MLML model and that can be managed as a single composite entity.

The present document specifies the AI/ML management related capabilities and services, which include the followings:

- AL/ML training.

- Sandboxing AI/ML

|  |
| --- |
| **Next modifications** |

## 6.N Sandboxing AI/ML

### 6.N.1 Description

Machine learning introduces an aspect of unpredictability in the network since there are no closed form descriptions for how the AI/ML Apps are supposed to work. As such, no one can confidently predict how the AI/ML Apps will perform in all possible contexts where they may be deployed. The AI/ML Apps will typically be trained offline (in the case of supervised learning-based functions) or may as such require a temporary environment from where to safely learn (e.g. for the case for reinforcement learning based functions).

AI/ML Apps that that rely on online learning, especially on reinforcement learning, need a non-intrusive environment for the training process. Such environment could be an emulator, a simulator, a test network or the real network under specified conditions. The ability to execute the AI/ML capability in any such controlled environment may be termed as sandboxing. The training and testing resources need to be reserved and configured for the particular use case, which can be a complicated task.

The AI/ML Apps may come from different vendors with different design philosophies and different AI/ML algorithms. This then requires that they are retrained and tested for the local context before they can be activated in the network.

As such, before deploying a function on the real network, the 3GPP management system needs a safe way to train and test the AI/ML Models to the local context and a mechanism to ensure that the function does exactly what has been promised, i.e. the system needs sandbox environments in which the function may be executed in a way that the cost of an unacceptable decision is minimized. Moreover, the 3GPP management system needs to orchestrate the execution of the AI/ML Apps to determine when to be executed on a sandbox, which particular sandbox is appropriate and when to be executed on the real system.

### 

### 6.N.2 Requirements

|  |  |  |
| --- | --- | --- |
| **Requirement label** | **Description** | **Related use case(s)** |
| **ML\_Sandbox\_Req\_1** | The 3GPP management system shall enable an authorized consumer to be informed by the producer of sandboxing services of the available sandbox environments, including but not limited to simulation environments, emulators, a digital twin of the network, a test network or a selected set of UEs for sandboxing purposes in the live network | Sandboxing AI/ML |
| **ML\_Sandbox\_Req\_2** | The 3GPP management system shall enable an authorized consumer to be informed by the producer of sandboxing services of the possible configurations of the available sandbox environments. | Sandboxing AI/ML |
| **ML\_Sandbox\_Req\_3** | The 3GPP management system shall enable an authorized consumer to request execution of an AI/ML App in a specific sandbox environment with specific configuration of the sandbox. | Sandboxing AI/ML |
| **ML\_Sandbox\_Req\_4** | The 3GPP management system shall enable the producer of sandboxing management services to configure the AI/ML Entities as need for specific sandbox environments, e.g. to control the allowed parameter space/ranges of the parameters optimized by the AI/ML App depending on the sandbox environment to which the parameters are being deployed | Sandboxing AI/ML |
| **ML\_Sandbox\_Req\_5** | The 3GPP management system shall enable using the real network as a sandbox under specific controlled conditions, e.g. only within certain hours or only on cells with load below a certain threshold or only on cells in a particular area or in limited subscriber groups. | Sandboxing AI/ML |
| **ML\_Sandbox\_Req\_6** | The 3GPP management system shall enable the producer of sandboxing management services to reconfigure the AI/ML Entities in operation in consideration of the observed behavior of the AI/ML Entities, e.g., to adjust the parameter space of the AI/ML Apps or to block the AI/ML Entity from being used on the network. | Sandboxing AI/ML |

|  |
| --- |
| **End of modifications** |