Exec model MQTT/TLS/JSON

Interface Design Description

Abstract
This document describes a MQTT protocol with TLS payload security and JSON payload encoding variant of the ”exec model” service.

Contents

1 Overview

This document describes the ”exec model” service interface, which provides the results of the inference using the AI model loaded in the AI-tool system and the dataset sent by the Preprocess system. The result is a boolean true if an intrusion was detected in the dataset analyzed by the AI-tool and false otherwise.

It’s implemented using protocol, encoding as stated in below table:

Profile ype	Type	Version
Transfer protocol	MQTT	1.1
Data encryption	TLS	1.3
Encoding	e.g. JSON	RFC 8259 [1]
Compression	N/A	-
Semantics	e.g. SensML	RFC 9100 [2]
Ontology	N/A	-

Table 1: Communication and sematics details used for the ”exec model” service interface

This document provides the Interface Design Description IDD to the *”exec model – Service Description* document. For further details about how this service is meant to be used, please consult that document.

The rest of this document describes how to realize the ”exec model” service interface in detail. Both in terms of its operations (Section 2) and its information model (Section 3).

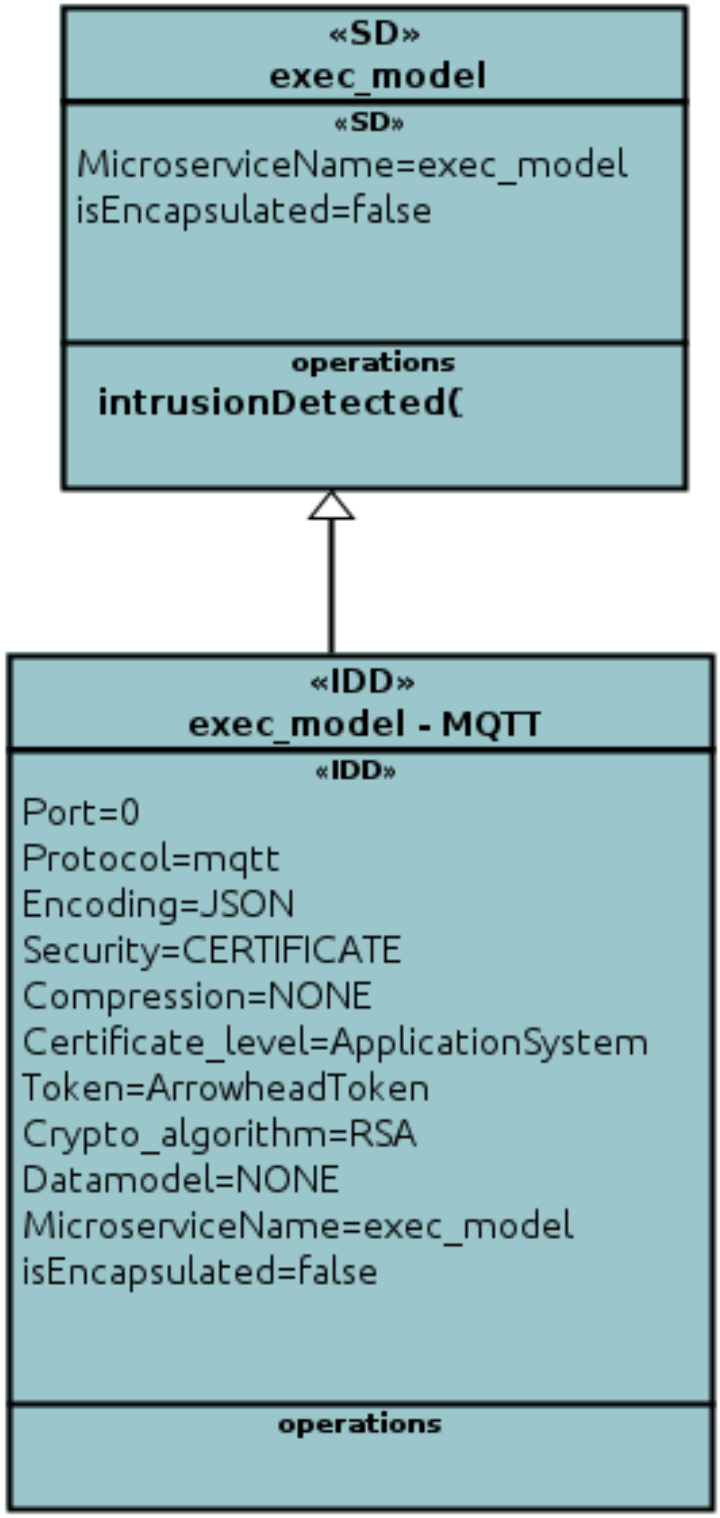

Figure 1: SysML model if the ServiceDIscovery interface, its operations, datamodels and implementation.

2 Service Operations

The interfaces of the ”exec model” service, its operations, data models and implementation are provided below. An SysML service overview is found in Figure 1.

In particular, each subsection first names the MQTT protocol method and path used to call the function, after which it names an abstract function from the exec model SD document, as well as input and output types.

All operations in this section respond with the status code `201 Created` if called successfully. The error codes are, `400 Bad Request` if request is malformed, `401 Unauthorized` if improper client side certificate is provided, `500 Internal Server Error` if Service Registry is unavailable.

2.1 MQTT Data Flow

The edge devices continuously monitor sensor readings and publish preprocessed data to the MQTT broker. The intrusion detection process consists of the following steps:

1. Preprocess system preprocess raw temperature data and send it to the central system via an MQTT topic (e.g., `sensor/data`).
2. The AI-tool system subscribes to the relevant topic and listens for incoming data.
3. Upon receiving the data, the system invokes the `exec-model` to run the machine learning model on the preprocessed data.
4. The model processes the data and returns an `intrusionDetected` flag indicating whether an intrusion has been identified.
5. The result is then published back to an MQTT topic (e.g., `alerts/warning`), informing other services of the detection.

2.2 POST /exec-model/intrusionDetected

Operation: exec-model
Input: preprocessedData
Output: intrusionDetected

Listing 2 demonstrates the registration of an example provider system using the MQTT-based architecture.

```
POST /ai-tool/exec-model HTTP/1.1
Host: example.com
Content-Type: application/json
Authorization: Bearer <token>

{
  "preprocessedData": {
    "version":1,
    "ipPackets": [
      {
        "sourceIP": "192.168.0.102",
        "destinationIP": "192.168.0.101",
        "payloadSize": 512,
        "timestamp": "2024-10-12T08:15:30Z"
      },
      ...
    ]
  }
}
```

Listing 1: `intrusionDetected`. invocation example

```
1
2 {
3   "version":1,
4   "intrusionDetected": False
5 }
```

Listing 2: `intrusionDetected`. response example

3 Data Models

Here, all data objects that can be part of the service calls associated with this service are listed in alphabetic order. Note that each subsection, which describes one type of object, begins with the *struct* keyword, which is meant to denote a JSON Object that must contain certain fields, or names, with values conforming to explicitly named types. As a complement to the primary types defined in this section, there is also a list of secondary types in Section 3.4, which are used to represent things like hashes, identifiers and texts.

3.1 struct preprocessedData

This structure is used to get the data and train the AI model.

Object Field	Value Type	Description
”ipPackets”	Array<ipPacket>	List of JSON objects containing IP headers.
”version”	Version	Version of the service.

3.2 struct intrusionDetected

This structure is used to notify the Alerts system that an intrusion was detected.

Object Field	Value Type	Description
”intrusionDetected”	Boolean	True if an intrusion was detected. False otherwise.
”version”	Version	Version of the service.

3.3 struct Metadata

A JSON Object which maps String key-value pairs.

3.4 Primitives

As all messages are encoded using the JSON format [3], the following primitive constructs, part of that standard, become available. Note that the official standard is defined in terms of parsing rules, while this list only concerns syntactic information. Furthermore, the Object and Array types are given optional generic type parameters, which are used in this document to signify when pair values or elements are expected to conform to certain types.

JSON Type	Description
Value	Any out of Object, Array, String, Number, Boolean or Null.
Object <A>	An unordered collection of [String: Value] pairs, where each Value conforms to type A.
Array <A>	An ordered collection of Value elements, where each element conforms to type A.
String	An arbitrary UTF-8 string.
Number	Any IEEE 754 binary64 floating point number [4], except for *+Inf*, *-Inf* and *NaN*.
Boolean	One out of `true` or `false`.
Null	Must be `null`.

With these primitives now available, we proceed to define all the types specified in the Service Discovery Register SD document without a direct equivalent among the JSON types. Concretely, we define the Service Discovery Register SD primitives either as *aliases* or *structs*. An *alias* is a renaming of an existing type, but with

some further details about how it is intended to be used. Structs are described in the beginning of the parent section. The types are listed by name in alphabetical order.

3.4.1 alias DateTime = String

Pinpoints a moment in time in the format of ”YYYY-MM-DD HH:mm:ss”, where ”YYYY” denotes year (4 digits), ”MM” denotes month starting from 01, ”DD” denotes day starting from 01, ”HH” denotes hour in the 24-hour format (00-23), ”MM” denotes minute (00-59), ”SS” denotes second (00-59). ” ” is used as separator between the date and the time. An example of a valid date/time string is ”2020-12-05 12:00:00”

3.4.2 alias id = Number

An identifier generated for each Object that enables to distinguish them and later to refer to a specific Object.

3.4.3 alias Interface = String

A String that describes an interface in *Protocol-SecurityType-MimeType* format. *SecurityType* can be SECURE or INSECURE. *Protocol* and *MimeType* can be anything. An example of a valid interface is: ”HTTPS-SECURE-JSON” or ”HTTP-INSECURE-SENML”.

3.4.4 alias Name = String

A String that is meant to be short (less than a few tens of characters) and both human and machine-readable.

3.4.5 alias SecureType = String

A String that describes an the security type. Possible values are *NOT_SECURE* or *CERTIFICATE* or *TOKEN*.

3.4.6 alias URI = String

A String that represents the URL subpath where the offered service is reachable, starting with a slash (”/”). An example of a valid URI is ”/temperature”.

3.4.7 alias Version = Number

A Number that represents the version of the service. And example of a valid version is: 1.

4 References

[1] T. Bray, “The JavaScript Object Notation (JSON) Data Interchange Format,” RFC 8259, Dec. 2017. [Online]. Available: https://rfc-editor.org/rfc/rfc8259.txt

[2] C. Bormann, “Sensor Measurement Lists (SenML) Features and Versions,” RFC 9100, Aug. 2021. [Online]. Available: https://rfc-editor.org/rfc/rfc9100.txt

[3] T. Bray, “The JavaScript Object Notation (JSON) Data Interchange Format,” RFC 7159, 2014, RFC Editor. [Online]. Available: https://doi.org/10.17487/RFC7159

[4] M. Cowlishaw, “IEEE Standard for Floating-Point Arithmetic,” *IEEE Std 754-2019 (Revision of IEEE 754-2008)*, July 2019. [Online]. Available: https://doi.org/10.1109/IEEESTD.2019.8766229

5 Revision History

5.1 Amendments

No.	Date	Version	Subject of Amendments	Author
1	2020-12-05	4.4.1		Szvetlin Tanyi
2	2021-07-14	4.4.1	Minor edits	Jerker Delsing
3	2022-01-17	4.4.1	Minor edits	Jerker Delsing

5.2 Quality Assurance

No.	Date	Version	Approved by
1	2022-01-17	4.4.1	Jerker Delsing