MLA Tool User Manual

Azadeh Sadat Mozafari Mehr
EINDHOVEN UNIVERSITY OF TECHNOLOGY | MATHEMATICS & COMPUTER SCIENCE, PROCESS ANALYTICS

1.Introduction

Existing conformance checking techniques focuses more on the control-flow perspective rather than other aspects in a business process. This may induce to misleading conformance diagnostics. MLA is a tool for multi-perspective conformance checking. In addition to control-flow perspective, this tool brings data and privacy perspectives' impact into conformance analysis to identify all intra- and inter-layer violations. Moreover, the tool can visualize the context in which data is processed and identify where data have been processed for unclear or secondary purposes by an authorised role. The tool has been implemented in the open source ProM framework. The provided user interface and graphical outputs make interpreting the conformance result simple.

2. Input

To run the MLA tool (Multi-layer Alignment plugin), 5 inputs are required:

1. A data model which relates the process logic to the data layer by indicating which data operations must be executed in order to complete a given activity (in csv format).
2. An organisational model which links users to their roles in csv format.
3. A process model with role information in PetriNet format.
4. A process log showing the start and complete of activities performed by specific resources in XES format.
5. A data Log in XES format

A sample of each models and required attributes for the logs are available at: https://github.com/AzadehMozafariMehr/MLATool.

2.1 Preparing Inputs

1. Data model:

- ✓ The data model contains two columns: Activity and data operation.
- ✓ The data model should be in "," delimiters CSV format.
- ✓ Each row shows one data operation. If the data operation has impact on more than one data field, the fields should be separated by "_" character.
- ✓ Activities with multiple data operations appear in multiple rows.

2. Organisational model

- ✓ The organisational model contains two columns: Role and User.
- ✓ The organisational model should be in "," delimiters CSV format.
- ✓ Users with multiple roles appear in multiple rows.

3. Process Model

- ✓ Make the process model in PetriNet format.
- ✓ Define the role of each activity in the label of activity in the process model. Separate the activity name and the role that is expected to perform the activity by ":" character in the label.

4. Process Log

- ✓ Prepare the process log in XES format
- ✓ A sample of the attributes of process events are:

```
<event>
        <string key="id" value="2"/>
        <string key="org:resource" value="R100"/>
        <string key="concept:name" value="Admission (ad)"/>
        <string key="lifecycle:transition" value="START"/>
        <date key="time:timestamp" value="1970-05-05T18:45:22.000+01:00"/>
</event>
<event>
        <string key="id" value="2"/>
        <string key="org:resource" value="R100"/>
        <string key="concept:name" value="Admission (ad)"/>
        <string key="lifecycle:transition" value="COMPLETE"/>
        <date key="time:timestamp" value="1970-05-05T19:47:07.000+01:00"/>
</event>
```

Note that start and complete events related to one instance of an activity should have the same id.

5. Data Log

- ✓ Prepare the data log in XES format
- ✓ A sample of the attributes of data events are:

```
<event>
        <string key="org:resource" value="D107"/>
        <string key="concept:name" value="Read:(AddmissionID,PatientID,MedicalHistoryID)"/>
        <string key="lifecycle:transition" value="COMPLETE"/>
        <date key="time:timestamp" value="1970-05-05T20:22:53.000+01:00"/>
</event>
```

2.2. Importing Inputs:

First, the inputs should be loaded into the PROM framework

Figure 1: ProM workspace

1. Press the import button (Fig.1)
2. Choose the required files to import:
    a. Select the data log and organizational models in ".csv" extension.
    b. Select the process model which is a Petri Net with ". pnml" extension.
    c. Select process log and data log in XES format with ". xes" extension.

Once you select a file and press open, you are prompted to select an import plugin. ProM automatically distinguishes the formats and shows a list of available import plugins for each input. Choose the default import plugin for each input.

At this stage, you can inspect the logs and its contents by applying the log view plugin as well as viewing the imported models using any the visualizers from the ProM framework by pressing the view button (Fig. 2).

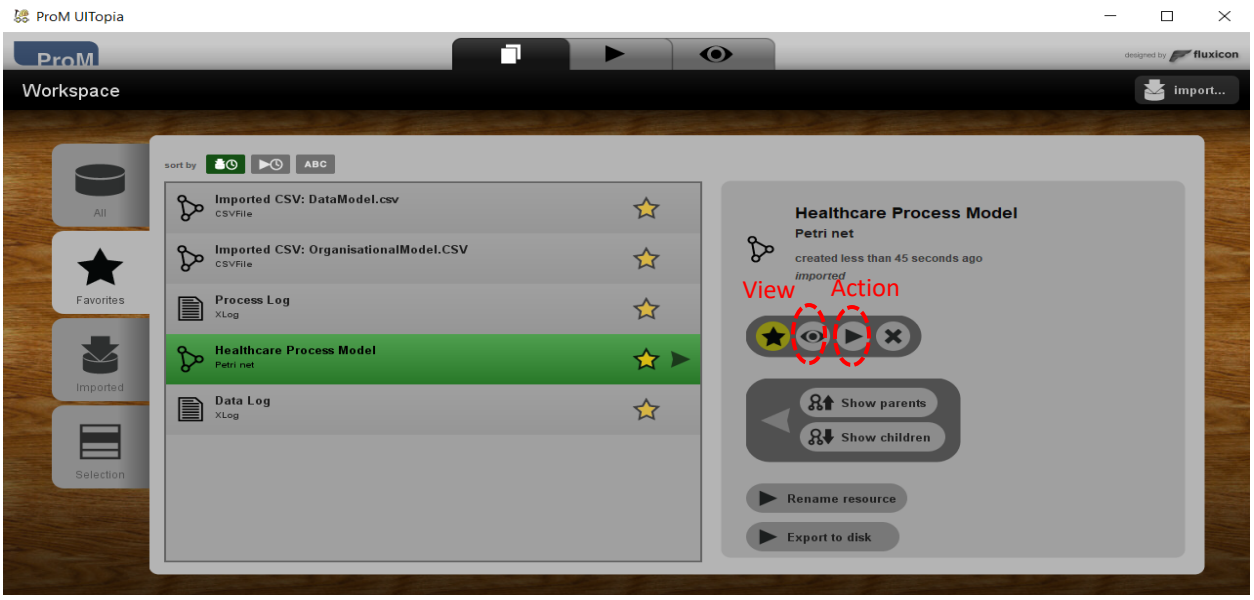

Figure 2:ProM workspace showing imported logs and models

3. Running

In order to run the MLA tool (Fig. 3).

1. Specify the inputs
    a. Switch to the 'Actions' tab (see Fig.2).
    b. Search for Multi-Layer Alignment in Actions panel to find and select the plugin.

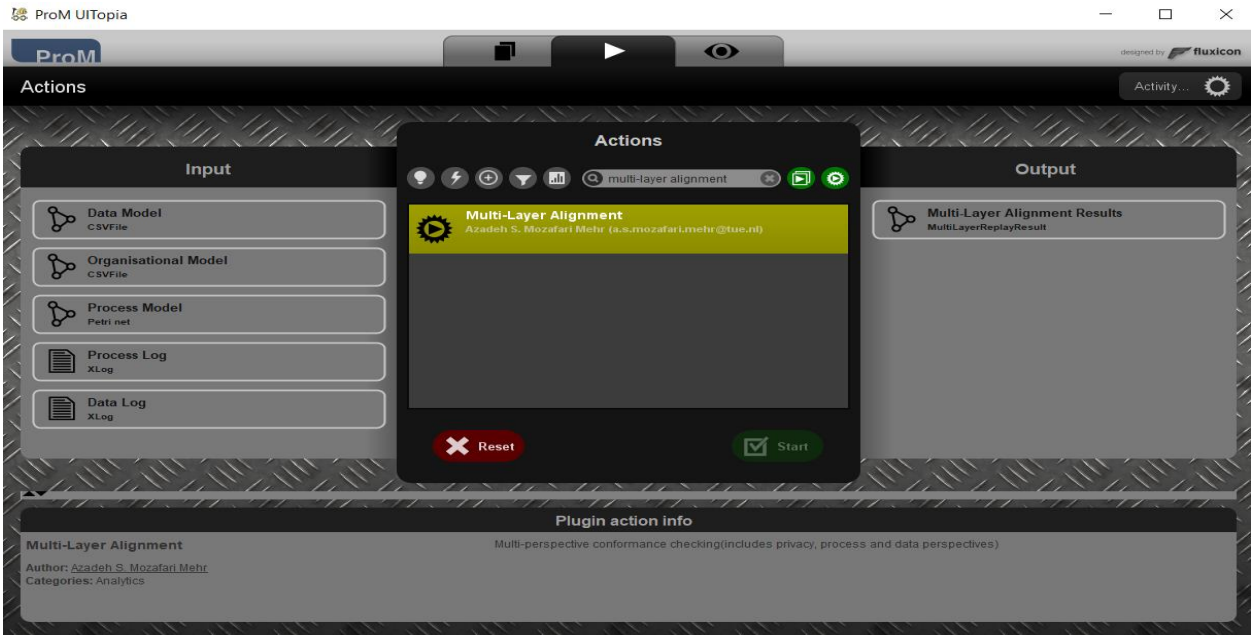

Figure 3: Action view of MLA plugin

c. On the input panel click on each required input and select the corresponding object from the provided list of the imported objects.
As shown in Figure 3, the order of the inputs is :1 Data Model, 2-Organisational model,3- process model, 4. process log and 5. Data Log. The first three inputs show modelled behaviour whereas process and data logs indicate observed behaviour.

2. Start the plugin
   a. After configuring the inputs in the right order, run the plugin by pressing the "start" button. During the alignment computations, progress is reported.

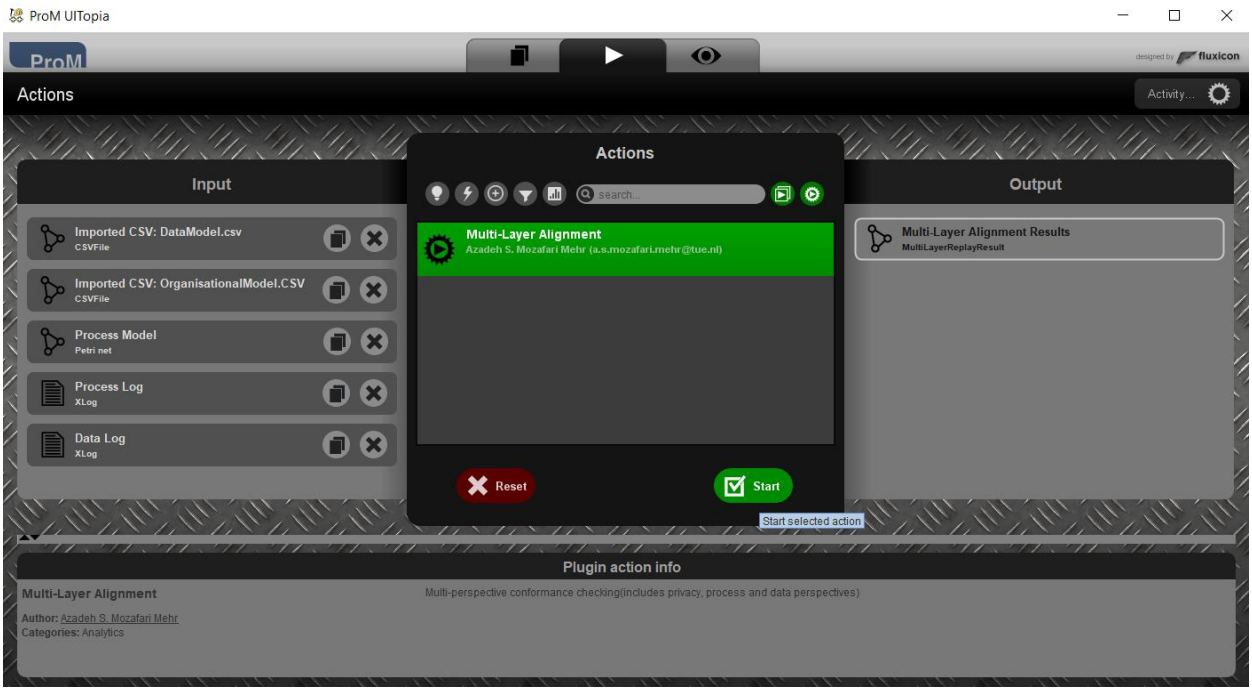

Figure 4: Running steps: After configuring the inputs run the MLA plugin by clicking start

b. The output of the plugin is a Multi-Layer alignment Results object, which will appear in the objects list after running the plugin

4. Visualisation

The plugin consists of two different visualisations called “Projection to Process Log” and “Projection to Data Log”. After completing the alignment computation, the result is by default projected on process log and the visualisation is shown as depicted in Fig.5.

4.1.Projection to Log Visualisation

Figure 5 shows a screenshot of “Projection to process log” visualisation. It includes two panels. In this visualisation ***privacy***, ***process***, and ***data*** perspectives are depicted by ***circles***, ***chevron arrows*** and ***triangles*** respectively

Figure 5: A screenshot of “Projection to process log” visualization

The right panel provides a guide for interpreting the result of multi-perspective conformance checking (Fig. 6).

Expected behaviours in each layer are shown in green color. Red color indicates unexpected behaviour and highlighted white/red color marks missing behaviour.

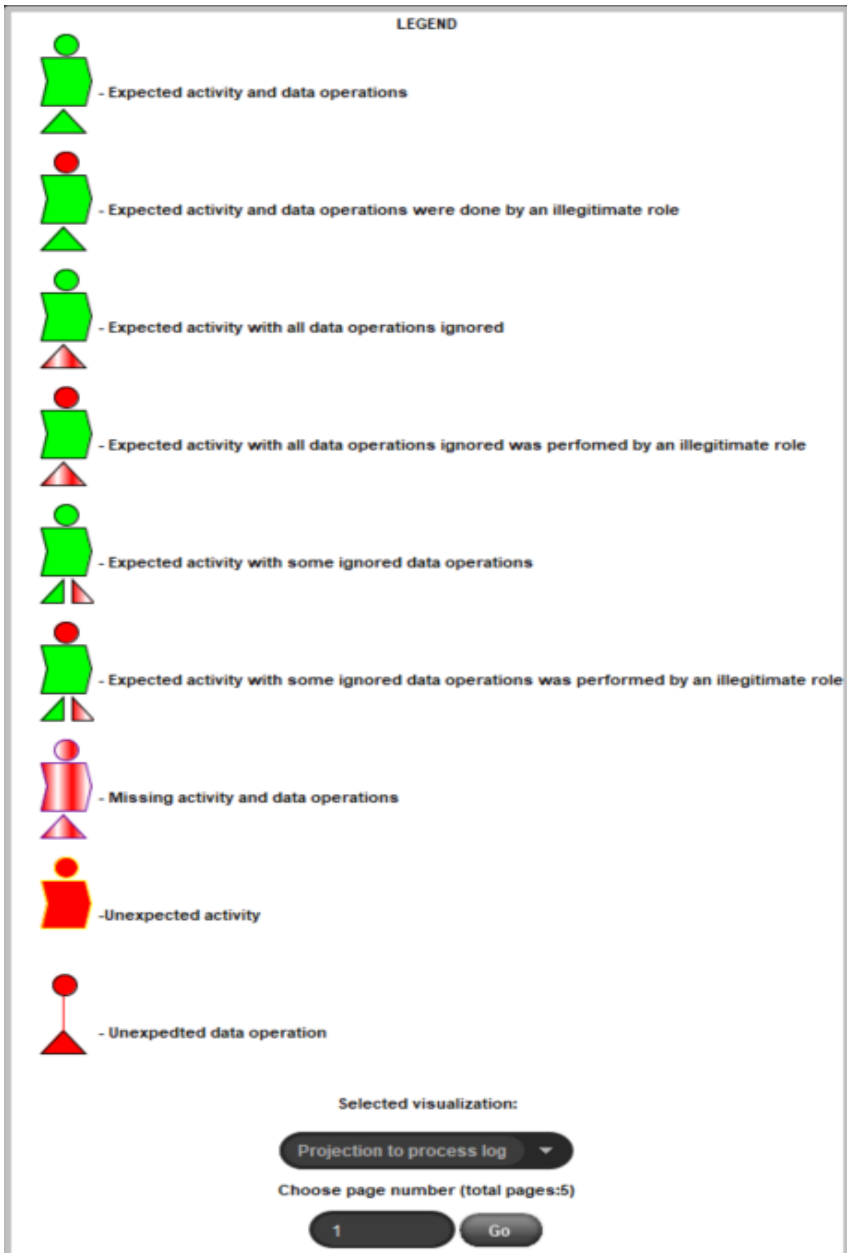

Figure 6: The legend of the "Projection to process log" visualization

The left panel is the main panel of the visualisation which provides operational insights and represents detected violations in the process, data, and privacy layers separately as well as inter-layer violations (see Fig. 5).

It enables observing the deviations of each aspect of a business process in an overall view per process instance (See Fig. 7). In this panel, privacy, process and data perspectives of each process instance are visualized by circles, chevron arrows and triangles respectively.

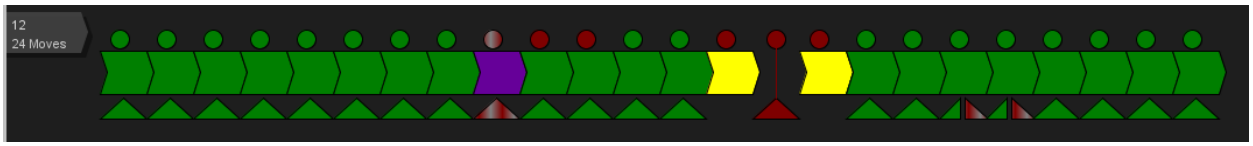

Figure 7: The overall view of one process instance from three perspectives

By clicking on each event, the visualizer indicates detailed information of the conformance analysis. (See Fig. 8).

Note that "#" means "the number of" in all visualizations.

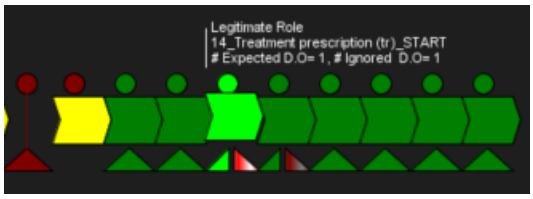

Figure 8: The process event flag shows detailed information about privacy, process, and data aspects in three lines respectively

The first line in the event flag reports the conformance result in the privacy aspect, the second line indicates the conformance of process (control-flow). The third line shows the conformance result of data operations in an overall view by showing the number of expected and unexpected data operations which were executed during the activity/task.

It can also show the activities with missing data operations and process events in which the actor didn't execute the required data operations during performing the activity (activities with ignored data operations).

Note that, in the control-flow based conformance checking techniques, purple and yellow colors are known as move on model and move on process log in the process mining research community.

We used these colors to show how our technique can detect hidden deviations related to other perspectives of a business process in addition to control-flow violations.

Figure 7 clearly shows that control-flow based conformance checking approaches can only detect the violations shown by purple and yellow colors while our approach is able to identify a larger range of hidden deviations.

In the developed tool, by clicking on model moves, purple color is changed to red/white color to indicate missing behaviour in all three perspectives of the process.

By clicking on the moves on process log, the yellow color is changed to red to mark unexpected behaviour from privacy and control-flow points of view.

4.2. Projection to data log Visualisation

On the top right, another visualisation can be chosen for the multi-perspective conformance result, namely “projection to Data log’, which shows the data aspect of the business process shown in Figure 9.

Figure 9: : A screenshot of “Projection to data log” visualization

The main panel of this visualisation indicates which data operations was executed during a process execution.

It shows expected data operations in green color and presents unexpected data operations in red color. Highlighted red/white color shows missing/ignored data operations.

The right panel in this visualisation provides a guide for interpreting the result of multi-perspective conformance checking from data and privacy aspects (Fig.10).

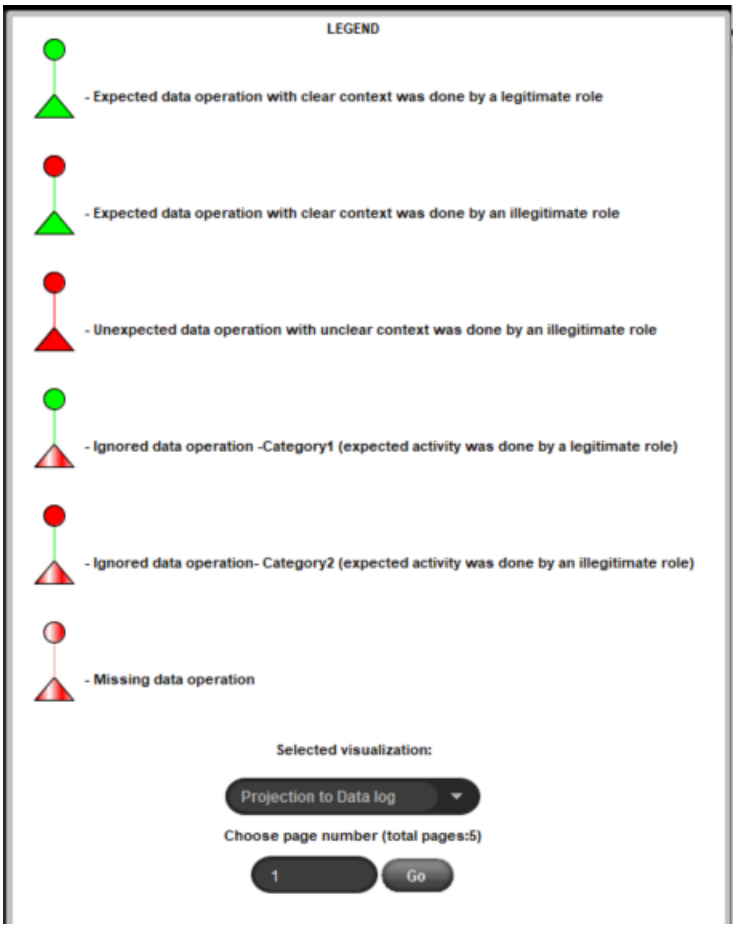

Figure 10: The legend of the "Projection to data log" visualization

This visualization enables detecting spurious data access and identify privacy infringements where data have been processed for unclear or secondary purposes by an authorized role. By clicking on each data event, the visualization shows the context of data processing and marks which data operations were executed with unclear or secondary purposes (see Fig. 11)

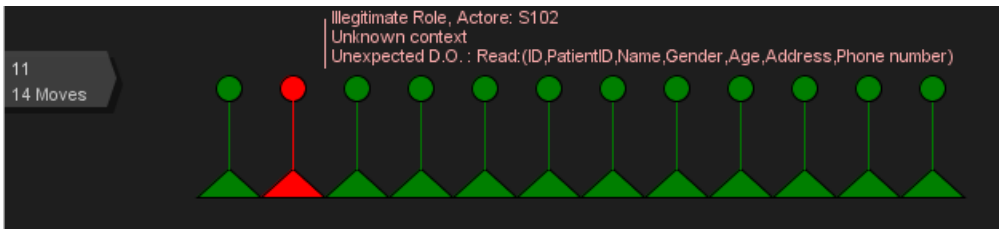

Figure 11: The data event flag shows the context of data processing and provides detailed information about privacy, data aspects