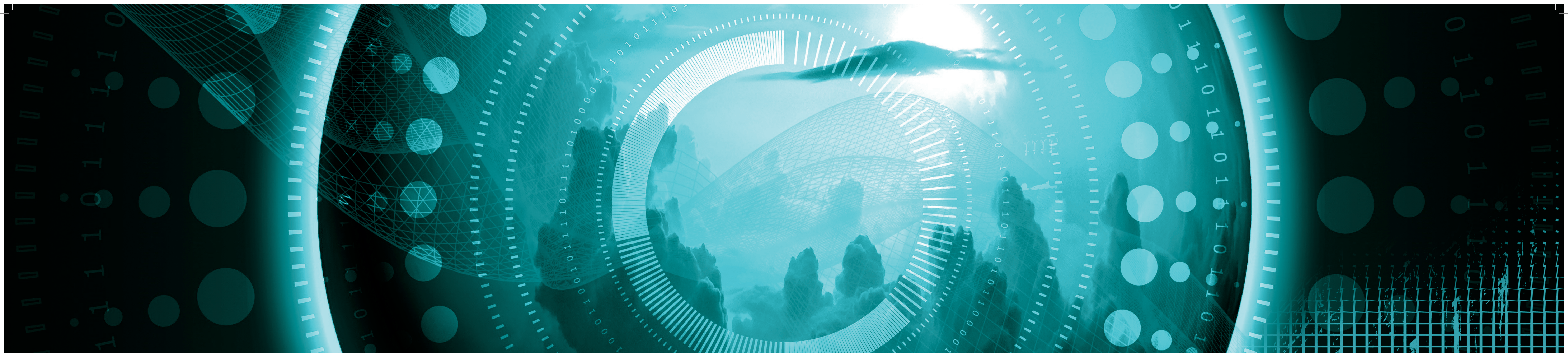


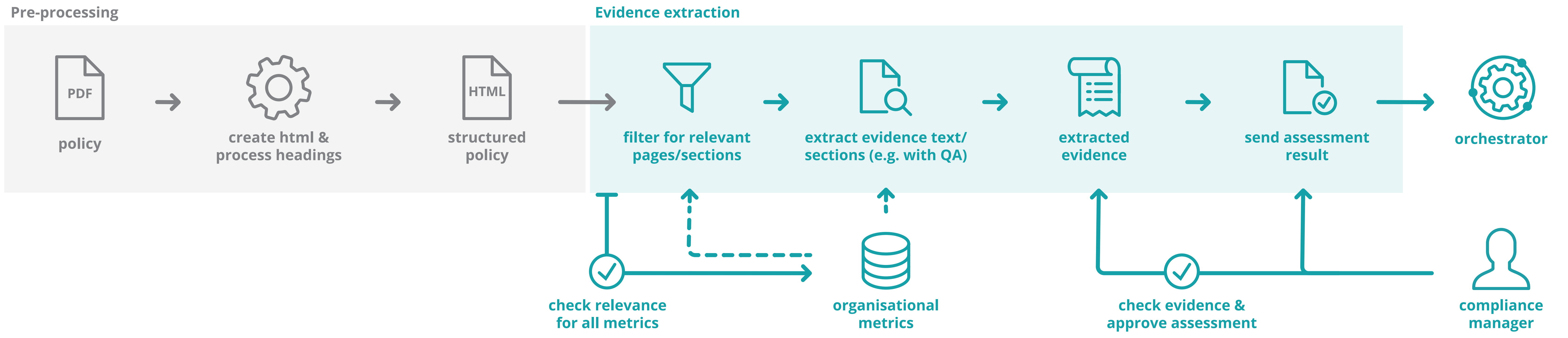
MEDINA

Assessment and Management of Organisational Evidence - AMOE

A Fabasoft component of the MEDINA project

Franz Deimling

Web: https://medina-project.eu/



Pre-processing
PDF
policy
create html & process headings
HTML
structured policy
Evidence extraction
filter for relevant pages/sections
extract evidence text/ sections (e.g. with QA)
extracted evidence
send assessment result
orchestrator
check relevance for all metrics
organisational metrics
check evidence & approve assessment
compliance manager

Figure 1: Architectual overview of the prototype

Objectives

The MEDINA project's AMOE component focuses on providing a solution that enables continuous and semiautomatic auditing for cloud service providers using the MEDINA framework.

Introduction

Cloud security schemes like the ENISA EUCS [1] include some controls and requirements that are of organisational nature, meaning they are not suitable to be automatically monitored in the way technical requirements are. Therefore, a subtask of the MEDINA project has been dedicated to finding a solution. The result of the related research activities is a simple prototype based on pretrained models. As MEDINA's assessment strategy for technical requirements is based on metrics, the approach was adapted to organisational requirements, resulting in the use of so-called organisational metrics. Each organisational metric consists of some keywords that are used to reduce the search space. The metric description is a simple question targeted to measure a specific feature commonly found in text documents relevant for audits. The metric target value is used to derive assessments hints that are provided to the compliance manager (user). The compliance manager or auditor needs to confirm (aided by an assessment hint if possible) that the extracted evidence fulfils the compliance status to an organisational metric. This can be done in an interactive GUI that displays the processed document as well as the original to double-check the information. Given well defined metrics, this could speed up the auditing process. The policy data processed is sensitive for the security of a cloud service, and thus large datasets are difficult to obtain. The relevant evidence text needs to be annotated for further training of new models and quality measurements of the prototype.

Data

The experiments and research conducted are based on unstructured textual policy data. The queries for the evidence extraction are based on the organisational metrics which are created specifically for the MEDINA project.

One example would be:

- **metric name:** LogDataRetentionTimeQ1
- **description**: How long is log data stored?
- **keywords**: logging, monitoring
- **scale**: days
- **operator**: <=
- **target value**: 100
- **data type**: int

Every security requirement of the EUCS is linked to multiple metrics that can be used to assess concrete parts defined in the rather generic requirements. Depending on the cloud service provider (CSP) and number of cloud services covered, policy documents can be very long (sometimes more than 50 pages). Therefore, to speed up processing time, the input data needs to be reduced, which can also lead to more precise results.

Pre-processing

MEDINA research discussions have shown that most of the CSP's policy documents are available as unstructured text documents (e.g. PDFs). To retain some of the structure given by elements like section headings, the PDF documents are pre-processed to HTML. Depending on the document origin, some headings need further rule-based recognition. This process is depicted in the left part of Figure 1.

Evidence extraction

The extraction of evidence snippets is based on a pre-trained question answering (QA) system (roberta-base-squad for QA[2]). The right part of Figure 1 shows the pipeline steps for evidence extraction. First, the input text document is filtered using the organisational metric keywords to reduce search space and thus processing time for the QA model. Then the selected sections are used to query the potentially relevant evidence text using the metric description (question). If the organisational metric has set a target value, the output of the model is translated into a similar format (if possible) and an assessment hint is computed by checking the output against the target value with the defined metric operator. The QA model provides a score that could aid in determining whether the output is relevant (not all queries produce relevant output). However, here is a promising research result for the example metric listed in the poster's data section (extracted answer in bold): „How long is log data stored?" Answer from QA: "From a operational necessity standpoint, we therefore configure the log retention time to a maximum of **90 days**, after which log data are automatically deleted."

Conclusion

The tool presented here could be a useful extension for any CSP to automate the auditing of textual policy documents. To make this tool future-proof, however, the challenge of creating a suitable dataset remains. In the future, other approaches such as text similarity can also be incorporated, as well as further research on pre-processing.

References

[1] ENISA EUCS – Cloud Services Scheme
https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme

[2] Question answering model - roberta-base-squad2
https://huggingface.co/deepset/roberta-base-squad2

Contact Information

Email: franz.deimling@fabasoft.com

This project has received funding from the European Union's Horizon 2020 research and innovation programm under grant agreement No: 952633.

Fabasoft®