



Co-Creating Misinformation- Resilient Societies

Generic Co-Inform Architecture – Version 1

D4.1

Document Summary Information

Project Title:	Co-Inform: Co-Creating Misinformation-Resilient Societies		
Project Acronym:	Co-Inform	Proposal Number:	770302
Type of Action:	RIA (Research and Innovation action)		
Start Date:	01/04/2018	Duration:	36 months
Project URL:	http://coinform.eu/		
Deliverable:	D4.1 Generic Co-Inform architecture – Version 1		
Version:	1.4 (Final version)		
Work Package:	WP4		
Submission date:	31/08/2018		
Nature:	P	Dissemination Level:	PU
Lead Beneficiary:	SCYTL SECURE ELECTRONIC VOTING		
Author(s):	Pau Julià, <i>Director of Security</i> (SCYTL)		
Contributions from:	David Salvador, <i>Technical Manager</i> (SCYTL) Adrià Rodríguez-Pérez, <i>Project Manager</i> (SCYTL) Oxana Casu, <i>Project Manager</i> (SU) Anton Haughey, <i>Developer</i> (SU) Stefan Nenzen, <i>Developer</i> (SU) Ipek Baris, <i>Researcher</i> (UKOB)		

The Co-inform project is co-funded by Horizon 2020 – the Framework Programme for Research and Innovation (2014-2020) H2020-SC6-CO-CREATION-2016-2017 (CO-CREATION FOR GROWTH AND INCLUSION).

Revision History

Version	Date	Change editor	Description
0.1	20/06/2018	SCYTL	Initial version
1.0	02/07/2018	SCYTL	FIRST DRAFT VERSION
1.1	14/08/2018	UKOB	First review
1.2	25/08/2018	SU	Second review
1.3	29/08/2018	SCYTL	Final version
1.4	31/08/2018	SU	Quality control and submission

Disclaimer

The sole responsibility for the content of this publication lies with the authors. It does not necessarily reflect the opinion of the European Union. Neither the Co-Inform Consortium nor the European Commission are responsible for any use that may be made of the information contained herein.

Copyright Message

©Co-Inform Consortium, 2018-2021. This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both. Reproduction is authorised provided the source is acknowledged.

Executive Summary

This report provides a first version of the architecture of the Co-Inform platform. It focuses on interoperability at business and information level, to be developed in an agile manner.

The system architecture of the Co-Inform project will be component-based and layered. Robustness, scalability and multi-user access support are important system characteristics. The architecture is designed based on general requirements from WP1 and its output will be a specification of the components of the system (coming from the research project partners in WP1 and WP3), how they interact (e.g., flows of control and data), and specification of programmable interfaces so that different partners can build their components independently. In addition to the components from the technical partners, the architecture provides infrastructural components required in the system's design, some examples being a data store, security (access control), and scheduling of automated tasks.

This deliverable will be complemented in three iterations (D4.2, D4.3, and D4.4), to be submitted respectively in M9, M15, and M21, which will feed from the on-going results from WP1, WP2 and WP3.

Table of Contents

1. Introduction.....	6
2. Co-Inform high-level architecture.....	7
2.1. Diagram	7
2.2. Components' description	8
i. Data collector (DC)	8
ii. Misinformation Detection (MD)	9
iii. Misinformation Flow Analysis and Prediction (MFAP).....	10
iv. Browser Plugin	11
v. Perception Flow and Behavior Mining (PBM).....	12
2.3. Data Flow	14
3. Conclusions.....	15

Table of Figures

Figure 1 High Level Architecture	7
Figure 2 Data Collector	9
Figure 3 Misinformation Detection	10
Figure 4 Misinformation flow analysis and prediction	11
Figure 5 Browser Plugin	12
Figure 6 Perception and Behaviour Mining.....	13
Figure 7 Data flow.....	14

1. Introduction

Misinformation online generates misperceptions. The speed and ease in which false news spread on social media have a massive impact on current affairs and policies. By bringing together a multidisciplinary team of researchers and experts in computer science, behavioural science, and sociology, Co-Inform aims to engage all stakeholders in fighting misinformation by providing them with the tools to identify ‘fake news’ online, understand how they spread, and provide them with verified information.

To this end, Co-Inform will integrate its ICT tools and services (WP3) and policy encodings (WP2) to deliver a co-created misinformation resilience platform in the form of:

- A browser plugin to raise citizens’ awareness of fully or partially misinforming content, of related fact checking articles and corrective information, of average citizens’ perceptions towards this content, and of key pro and against comments from fellow citizens.
- A dashboard for fact checking journalists and policymakers, showing that misinformation was detected, where originated from, how and where it has spread and will spread in the near future, what’s the current and predicted public perception, and what are the key comments about it from the public. The dashboard will also show the news articles or information that users requested to be fact checked.

This deliverable describes the high-level architecture of the Co-Inform platform, including the interaction between its expected components.

This is a preliminary version of the architecture, which will be revised, updated and detailed as required in order to comply with the set of requirements gathered with the Platform’s end-users in the course of the activities within WP1, with the management policies from WP2 and with the services developed in WP3. Specifically, it will be updated in three iterations (D4.2, D4.3, and D4.4), to be submitted respectively in M9, M15, and M21.

2. Co-Inform high-level architecture

2.1. Diagram

The following diagram illustrates the high-level architecture proposed for the Co-Inform platform:

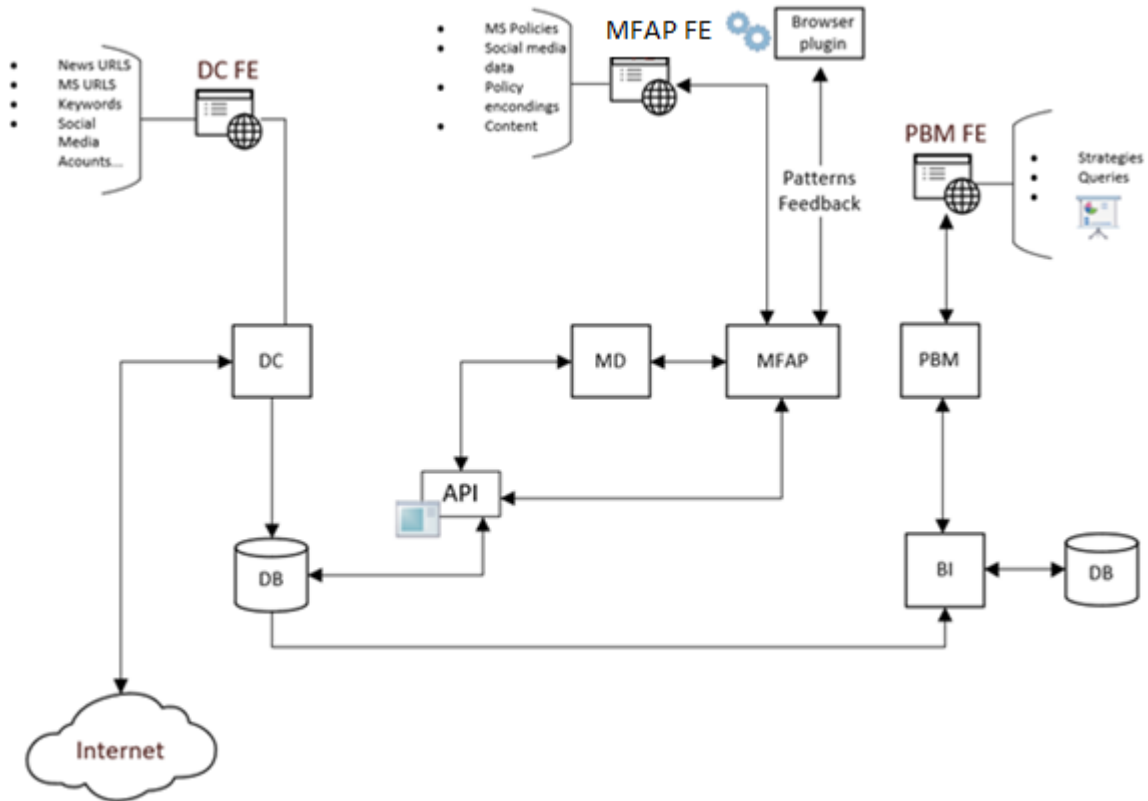


Figure 1 High Level Architecture

API: Application Programming Interface
 BI: Business Intelligence
 DB: Database
 DC: Data Collector
 DC FE: Data Collector Front End
 MD: Misinformation Detection

MFAP: Misinformation Flow Analysis and Prediction
 MFAP FE: Misinformation Flow Analysis and Prediction Front End
 PBM: Perception Behaviour Mining
 PBM FE: Perception Behaviour Mining Front End

2.2. Components' description

The following components will be needed to implement the Co-Inform architecture, based on the technical proposal submitted to the European Commission.

Some of these components could be integrated into a single component or some of them could be split in other modules. These modules must be understood as a baseline to implement a more detailed infrastructure once the requirements are defined.

i. Data collector (DC)

The **Data Collector** is the module in charge of collecting the information that will be processed using ESI's industry-leading text analytics technology. This module will collect multilingual content from the Web. The addresses, URLs, and different sources of data like news, misinformation generation sites keywords and social media accounts will be managed via a web front-end that will administrate the configuration of this module.

This module will require:

- Database

This module needs a database to store all the collected data to feed the next module that will detect the misinformation.

The internal data structures of this database will be defined and detailed in next architecture versions.

This database must be encrypted and the information it contains anonymised when possible, to guarantee the security of the personal information and to be GDPR-compliant.

This module might write directly to the Database or go through the API (see below).

- API interface

In turn, this data base will need an **API interface** to facilitate the access of this database by the other components.

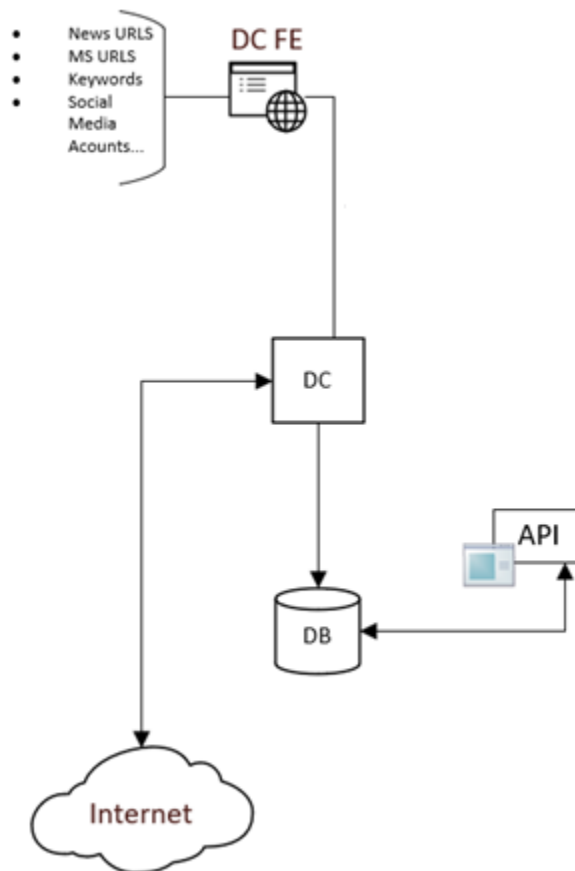


Figure 2 Data Collector

ii. Misinformation Detection (MD)

Misinformation Detection is the module in charge to analyse the data collected by the **Data Collector** and find misinformation data.

This module will use intelligent algorithms for measuring misinformation-probability of text articles and their sources, and to rank them based on their relative importance using a mixture of supervised and unsupervised models.

The detection algorithm will follow relevant policies entered via a web front end that could be shared with the **Misinformation Flow Analysis and Prediction Module (see section 3.2.3 below)**. Historical data into the Data Base will be reached via the API developed into the previous module and it will be used to train and test these models, which will be produced using content, temporal, semantic, network, and user features. The Data Collector might write directly to the Database or go through the API.

This module will be connected and will work together with the **Misinformation Flow Analysis and Prediction module**

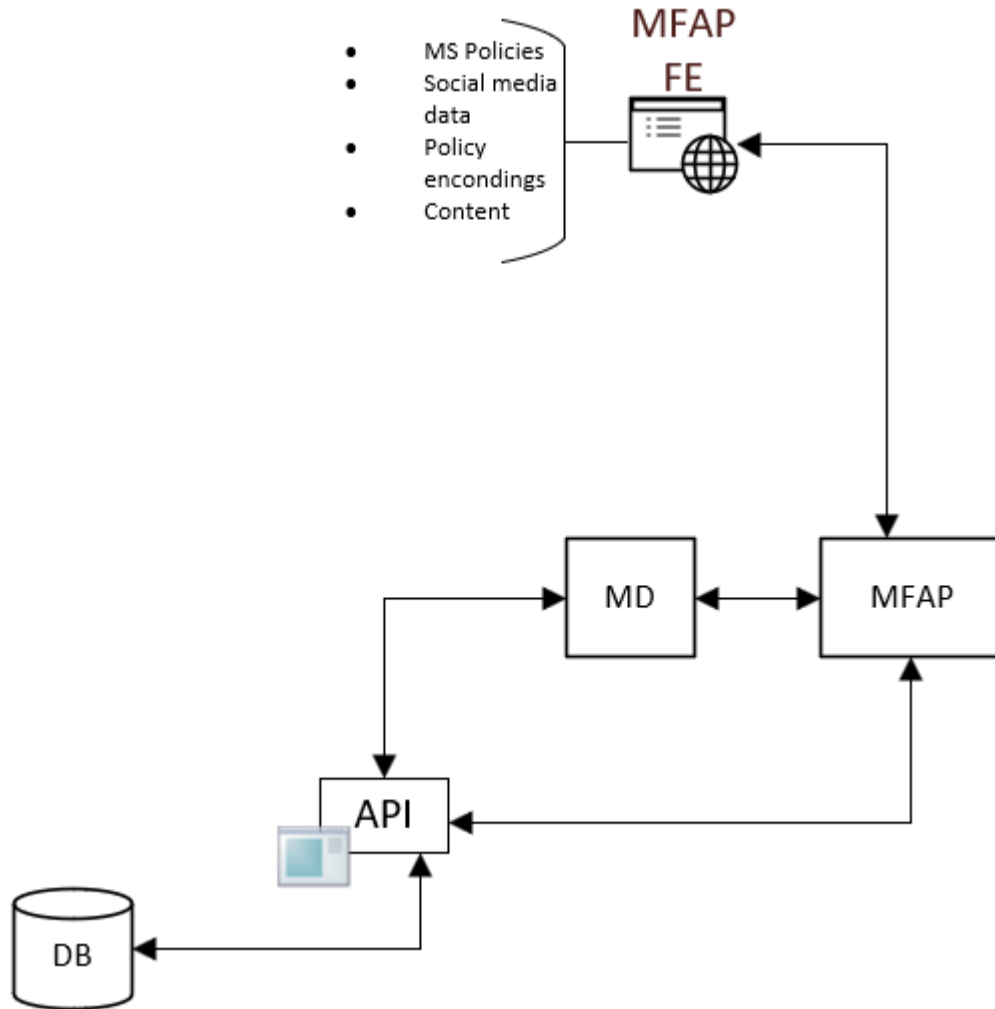


Figure 3 Misinformation Detection

iii. Misinformation Flow Analysis and Prediction (MFAP)

This module will work together with the **Misinformation Detection** module using the historical data collected and determine patterns of different types of misinformation across the social networking platforms analysed. This patterns recognition will use different parameters that could be managed via the shared web front-end with the **Misinformation**

Detection module. These parameters could be understood as policies (following the wording in the proposal for the activities under WP2).

This module will feed the next module in discussion, that is the web browser plugin. The type and kind of information that will be used to manage the plugin will be defined in the following versions of the Platform's Architecture Design.

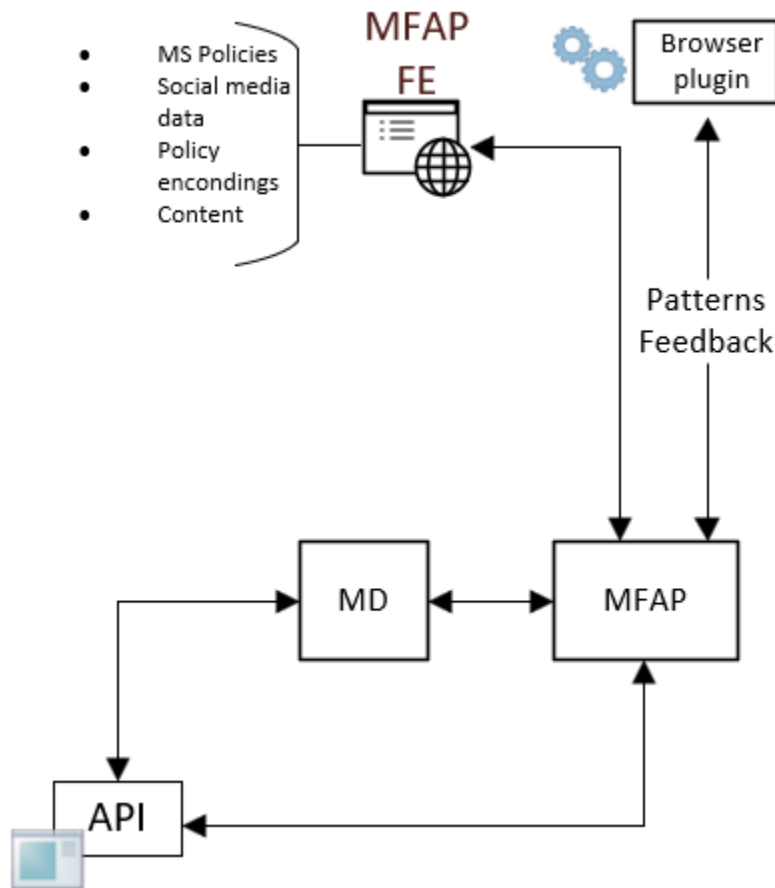


Figure 4 Misinformation flow analysis and prediction

iv. Browser Plugin

This module will be the end user module (i.e. for social media users). It will analyse the end user navigation and together with the patterns provided by the **Misinformation Flow Analysis and Prediction** module will inform about the credibility of the information that they are accessing to.

An output can be generated with the interaction and possible validation and classification of the information tagged by the user. This output must be acquired completely anonymised and the channel used must be encrypted (e.g. using TLS). This output will be managed by the **MFAP** to enforce the misinformation detection.

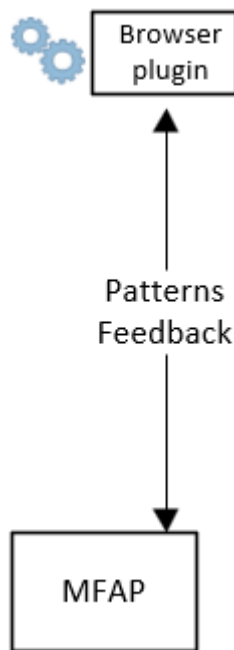


Figure 5 Browser Plugin

v. Perception Flow and Behavior Mining (PBM)

Using the information stored into the data base, the analysis and classification conducted by the **MD** module and the **MFAP** module and using the statics and reactions collected by the **browser plugin**, this module will provide statistics on misinformation behaviours.

The core of this module is planned to be managed by a Business Intelligence service/application using an alternative database, which will be feed periodically by the central database (3.2.1). The adoption of this approach will boost a performance increase of the overall system.

This module will provide dashboards and statistics about the misinformation managed within the whole system. The specific parameters of each end user will be inputted into the PBM through a web front end.

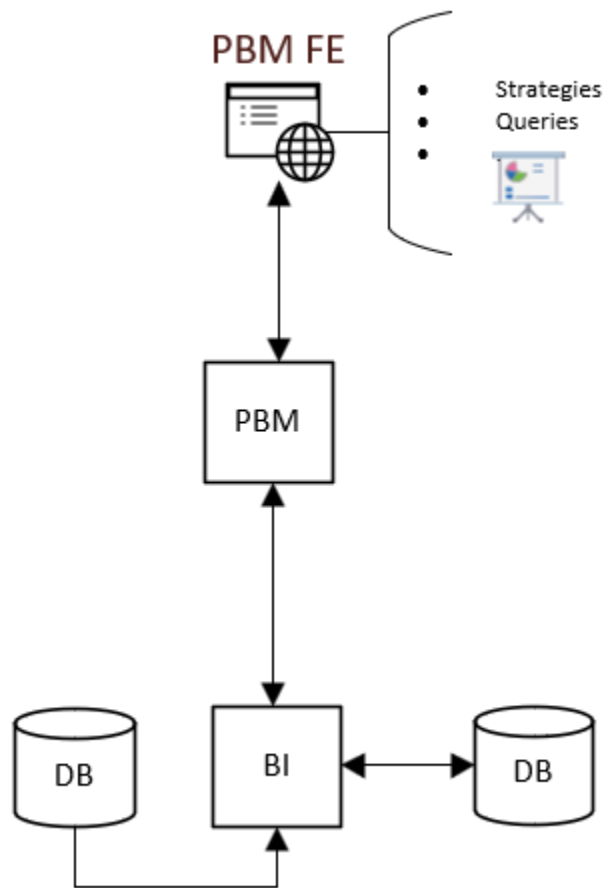


Figure 6 Perception and Behaviour Mining

2.3. Data Flow

The following diagram depicts the data flown between the different components:

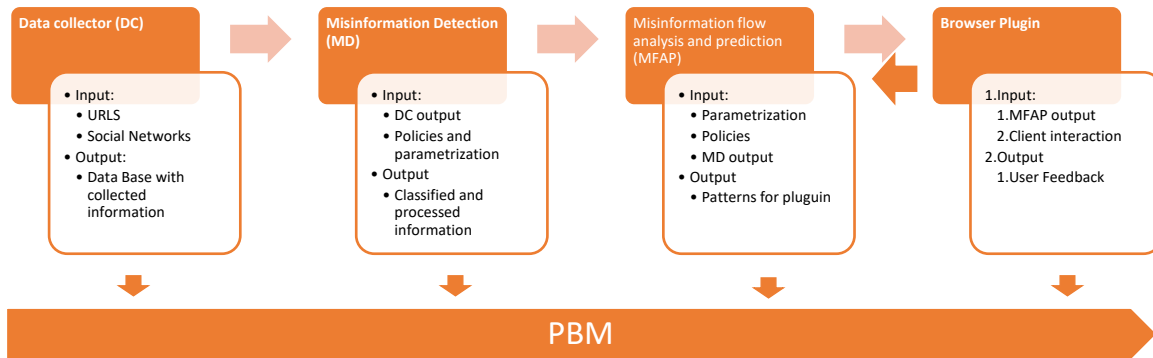


Figure 7 Data flow

3. Conclusions

This deliverable describes the high-level architecture of the Co-Inform platform, including the interaction between its expected components. Specifically, it provides a high-level specification for the platform components and their expected interaction, namely:

- Data Collector (DC)
- Misinformation Detection (MD)
- Misinformation Flow Analysis and Prediction (MFAP)
- Browser Plugin
- Perceptions and Behaviour Mining (PBM)

This is a preliminary version of the architecture, which will be revised, updated and detailed as required in order to comply with the set of requirements gathered with the Platform's end-users in the course of the activities within WP1, with the management policies from WP2 and with the services developed in WP3. Specifically, it will be updated in three iterations (D4.2, D4.3, and D4.4), to be submitted respectively in M9, M15, and M21.

Specifically, future versions of this deliverable should also specify:

- Specification of components
- Workflow and integration of components
- API documentation
- Hosting architecture

