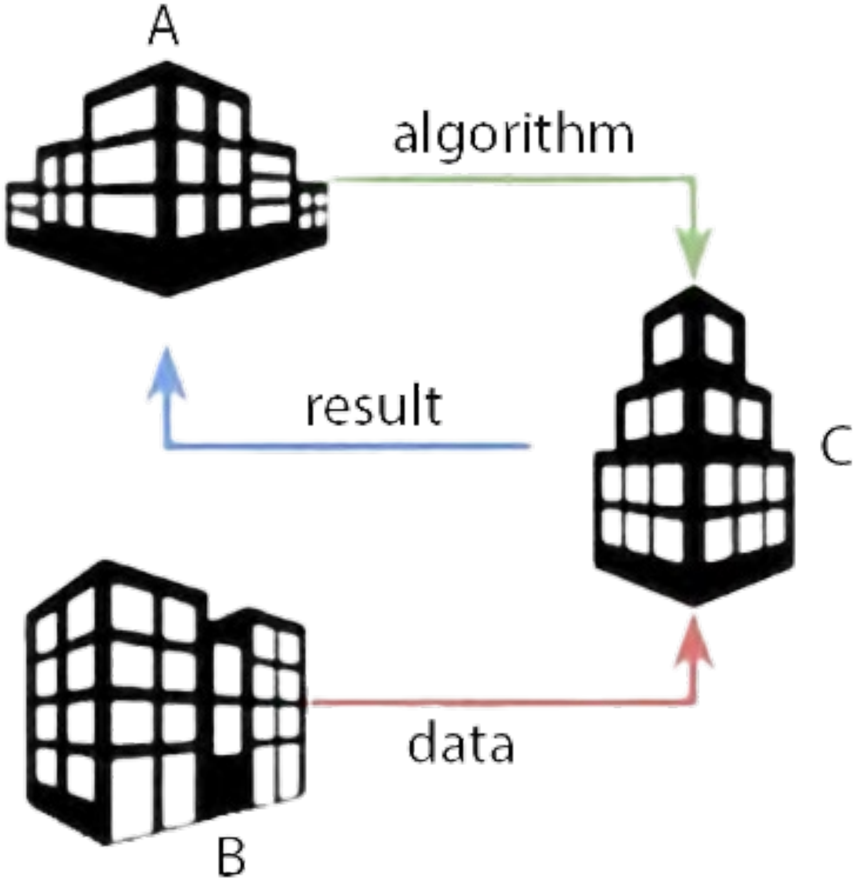
UNIVERSITEIT VAN AMSTERDAM

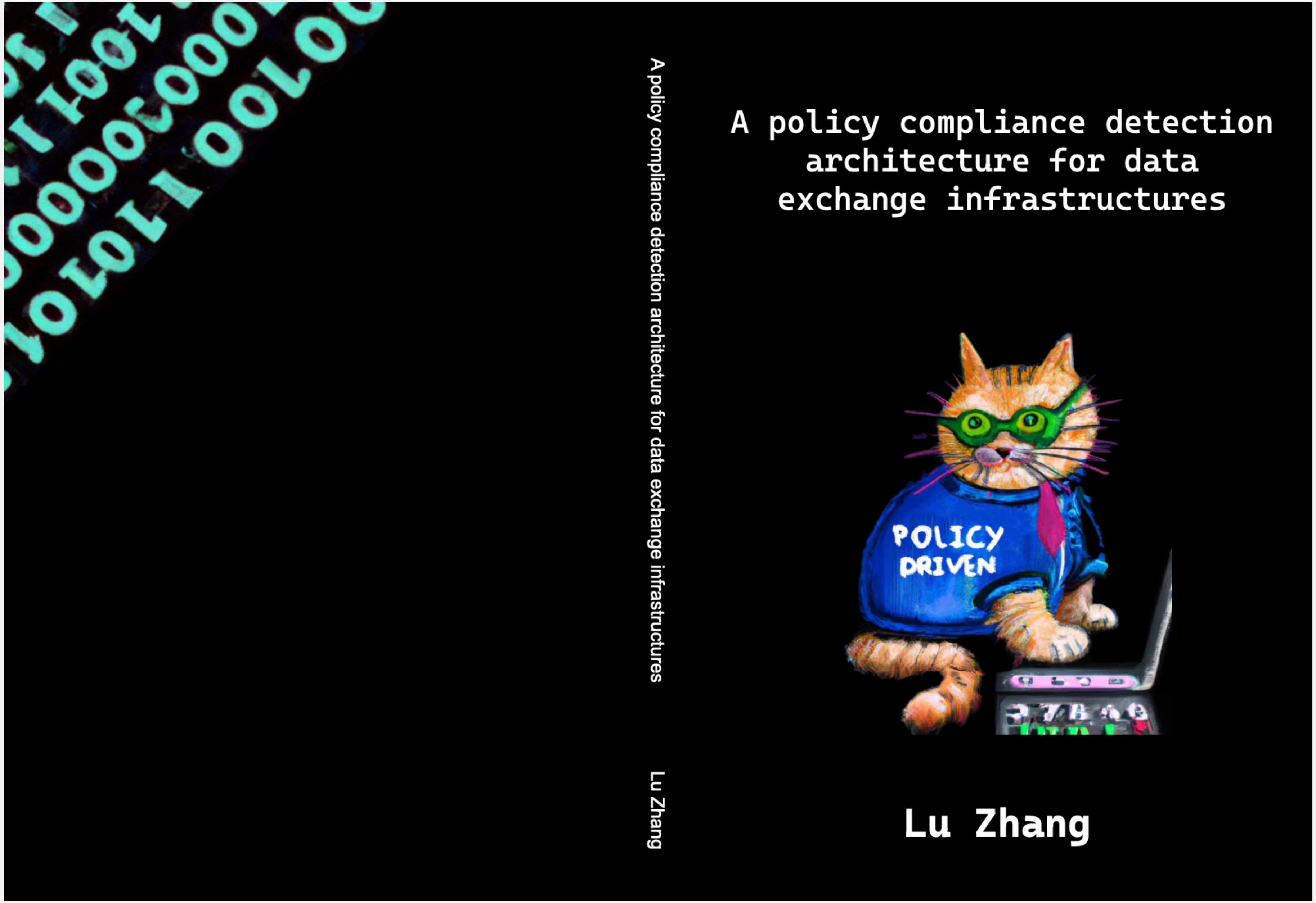
Generating a compliant normative controlled cloud data sharing infrastructure



Dr. Paola Grosso

On behalf of **dr. Lu Zhang**

And contributions from dr. R.Cushing, dr. A. Taal, dr. R. Koning, prof. L Gommans and prof. C. de Laat



A policy compliance detection architecture for data exchange infrastructures

Lu Zhang

A policy compliance detection architecture for data exchange infrastructures

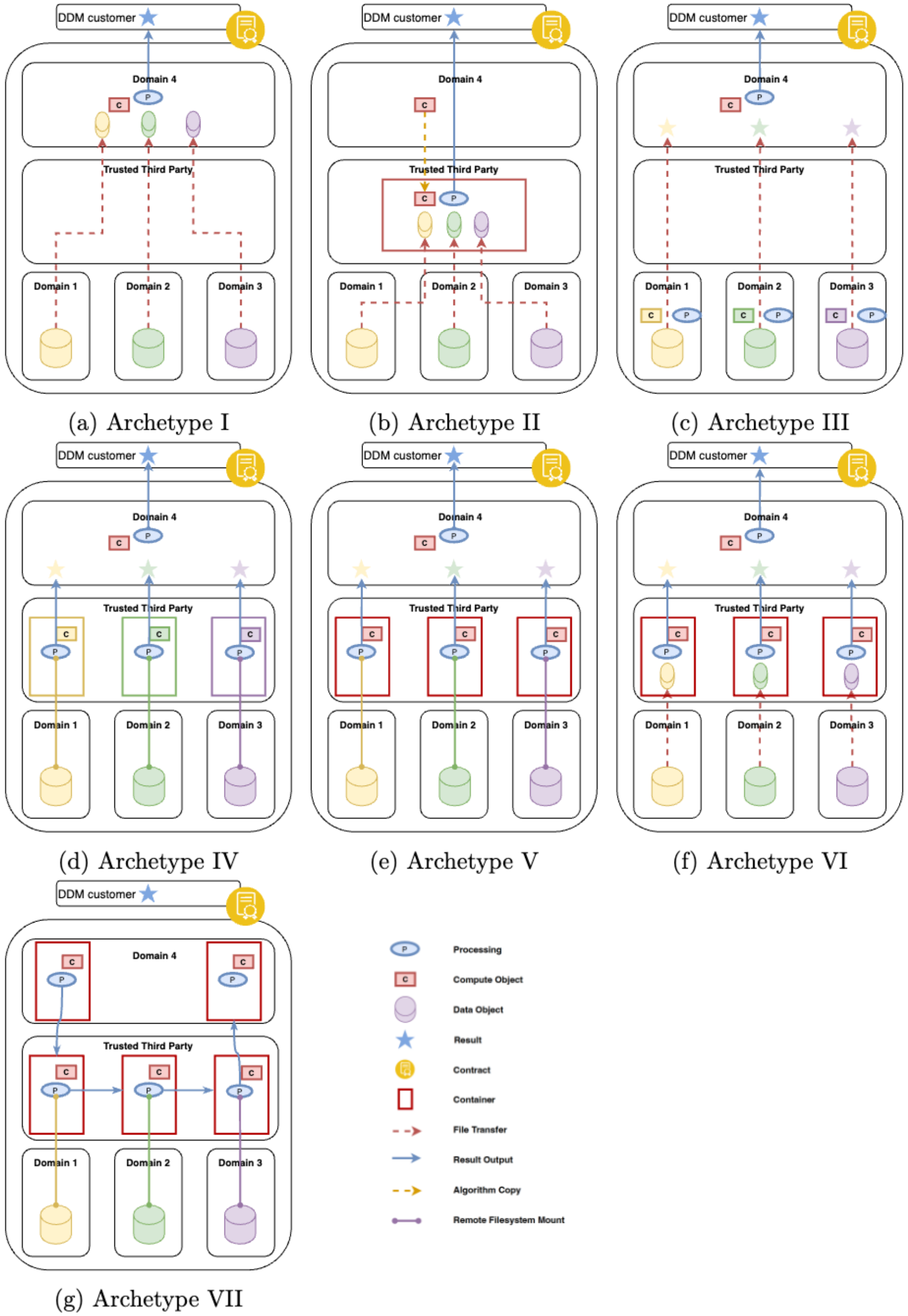
Lu Zhang

More information?

- Lu Zhang, Reginald Cushing, Leon Gommans, Cees De Laat, and Paola Grosso, “Modeling of collaboration archetypes in digital marketplaces” in journal IEEE 1.3. Publications 7 Access, DOI: 10.1109/ACCESS.2019.2931762.
- Lu Zhang, Arie Taal, Reginald Cushing, Cees de Laat, Paola Grosso, “A risk level assessment system based on the STRIDE/DREAD model for Digital Data Marketplaces” in journal International Journal of Information Security.
- Lu Zhang, Reginald Cushing, Ralph Koning, Cees de Laat, Paola Grosso, “Profiling and discriminating of containerized ML applications in Digital Data Market places (DDM)” In: 7th International Conference on Information Systems Security and Privacy (ICISSP 2021).
- Lu Zhang, Reginald Cushing, Cees de Laat, Paola Grosso, “A real-time intrusion detection system based on OC-SVM for containerized applications” In: 24th IEEE International Conference on Computational Science and Engineering (CSE 2021).
- Lu Zhang, Reginald Cushing, Paola Grosso, “Defending OC-SVM based IDS from poisoning attacks” , the 5th IEEE Conference on Dependable and Secure Computing (IEEE DSC 2022)

UNIVERSITEIT VAN AMSTERDAM

Archetypes



(a) Archetype I

(b) Archetype II

(c) Archetype III

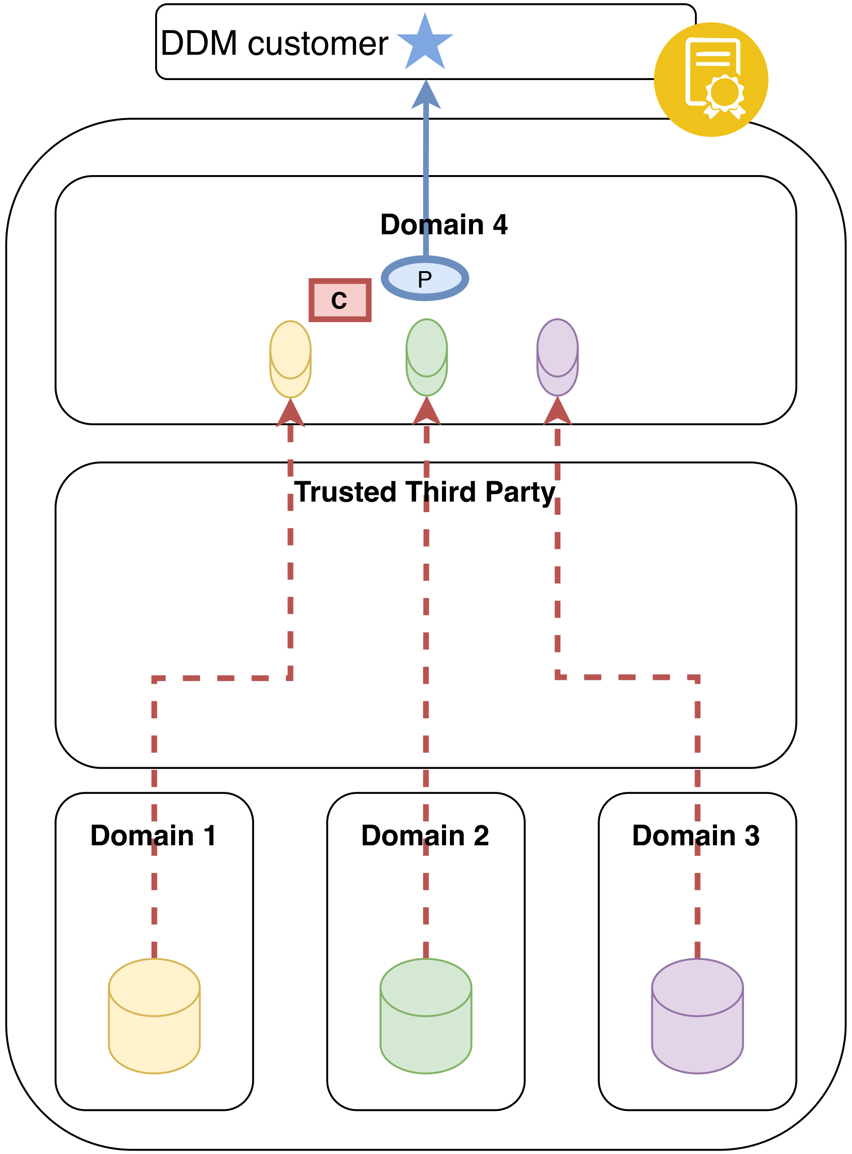
(d) Archetype IV

(e) Archetype V

(f) Archetype VI

(g) Archetype VII

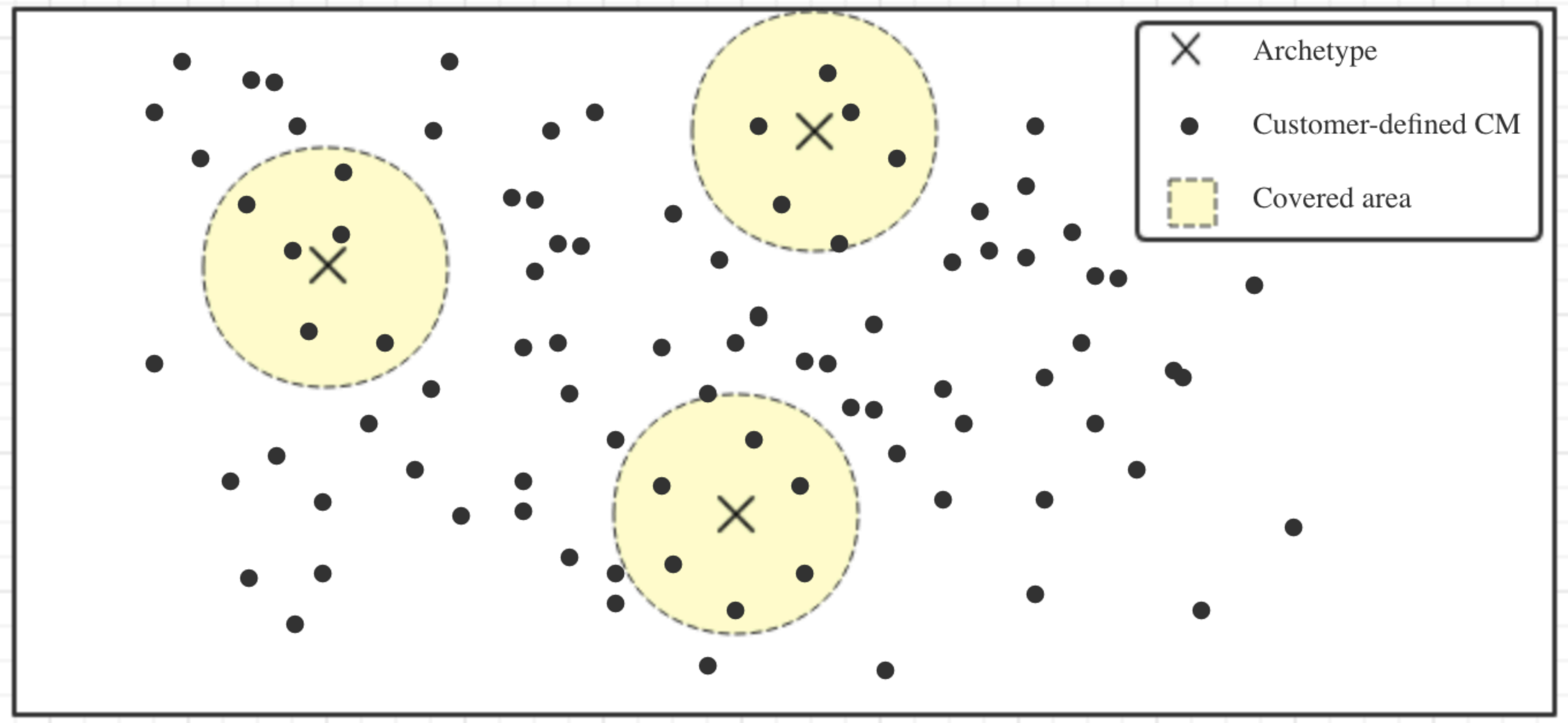
Zoom in



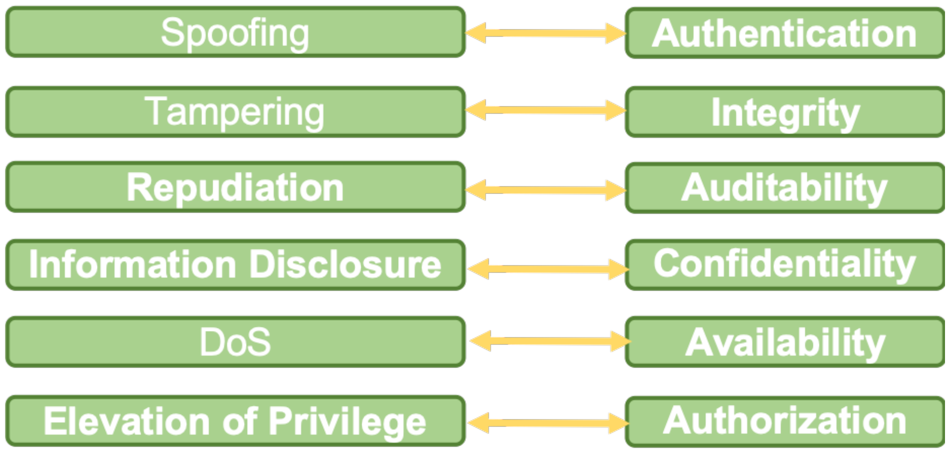
P	Processing
C	Compute Object
⛁	Data Object
★	Result
●	Contract
□	Container
- -➤	File Transfer
⟶	Result Output
- -➤	Algorithm Copy
●—●	Remote Filesystem Mount

Coverage

How to map an application request to a best-fit digital infrastructure
pattern based on collaboration models?

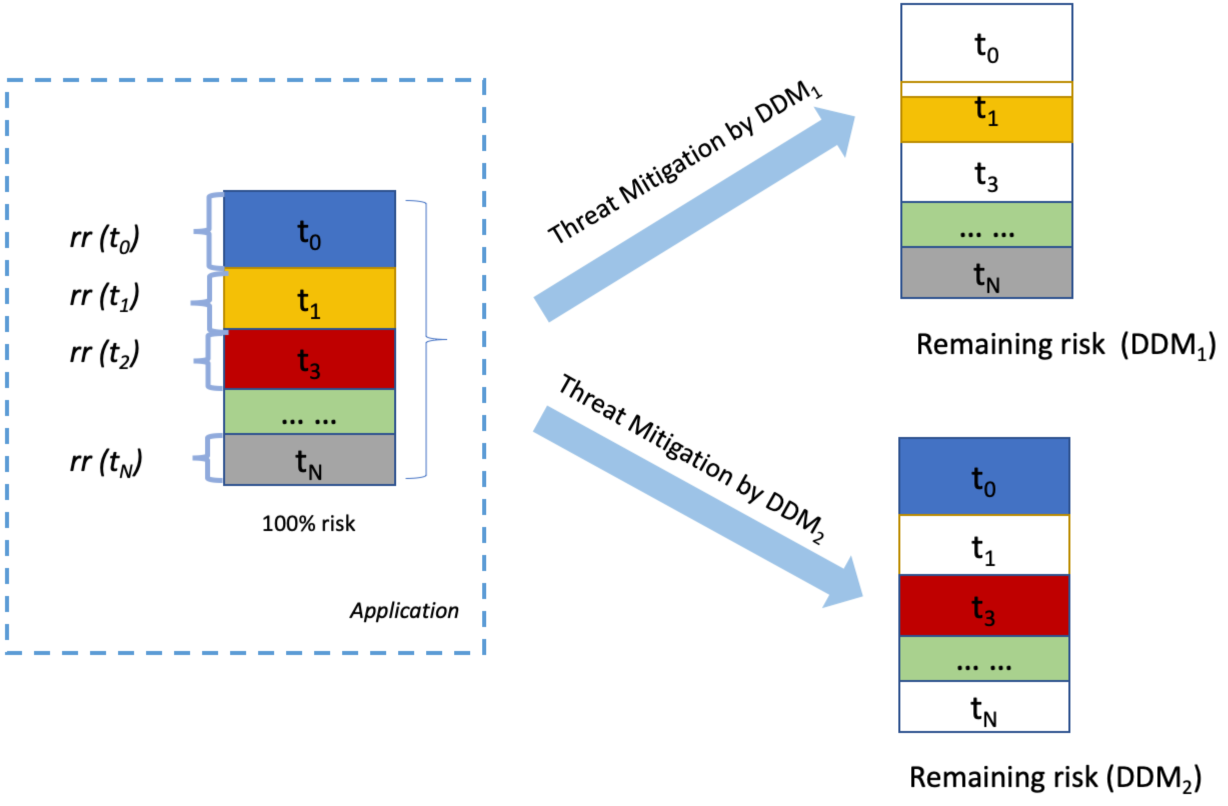


Risk assessment



Spoofing	Authentication
Tampering	Integrity
Repudiation	Auditability
Information Disclosure	Confidentiality
DoS	Availability
Elevation of Privilege	Authorization

How to select an optimal digital infrastructure with minimum risk?

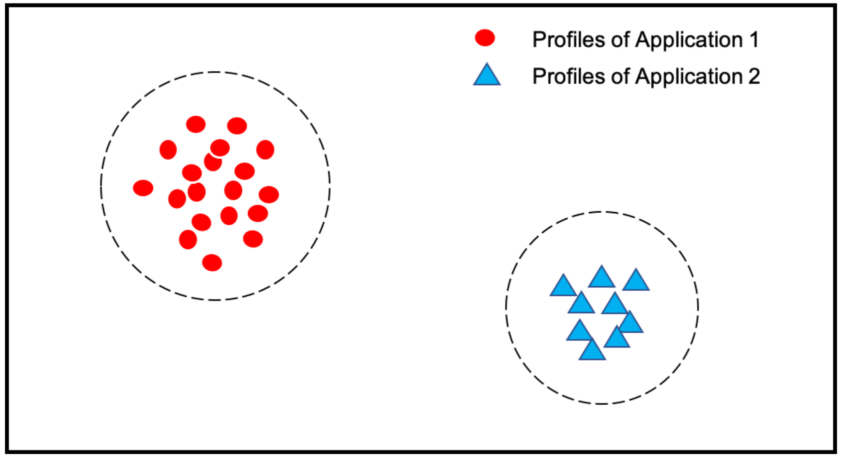


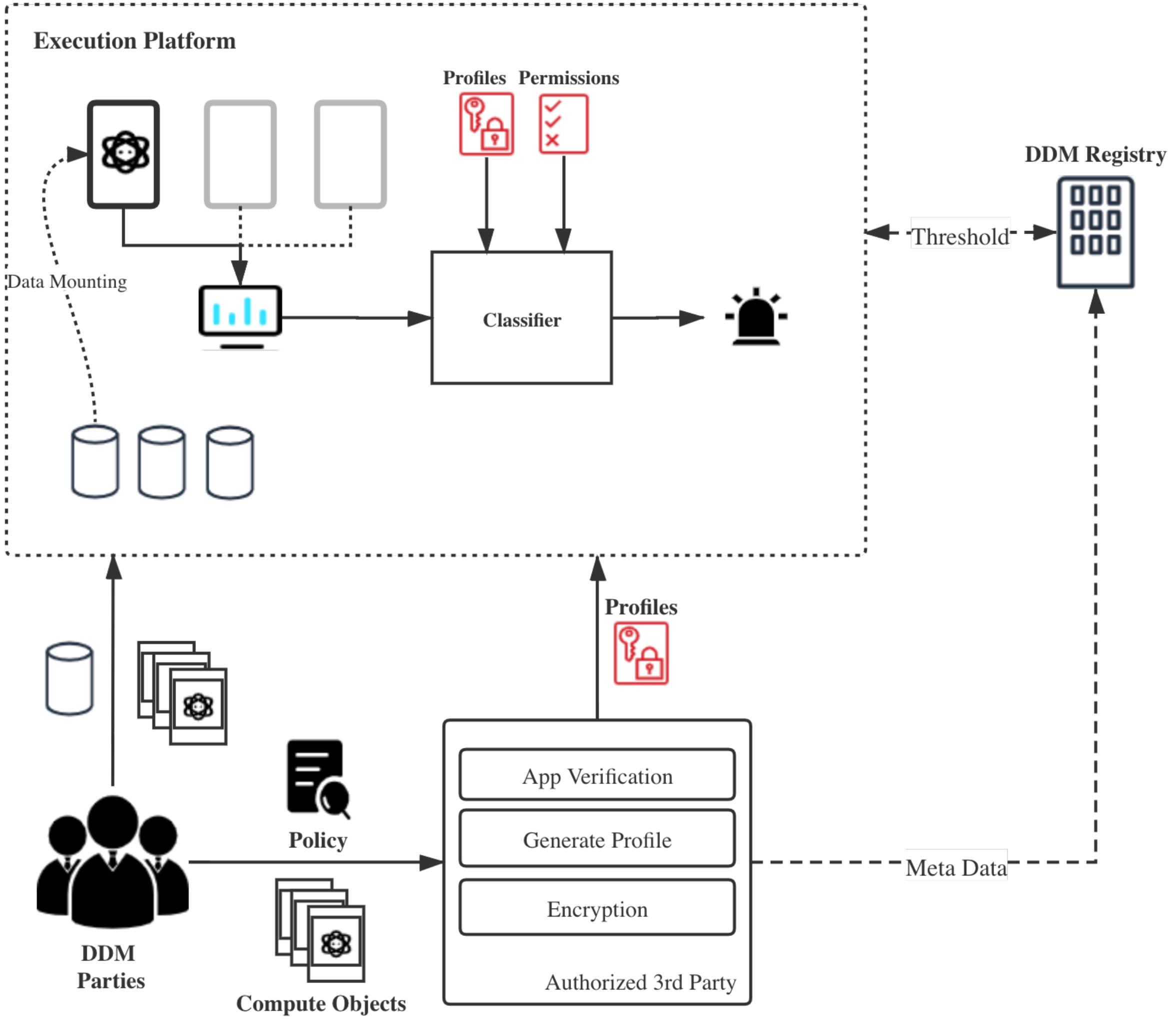
Remaining risk (DDM_1)

Remaining risk (DDM_2)

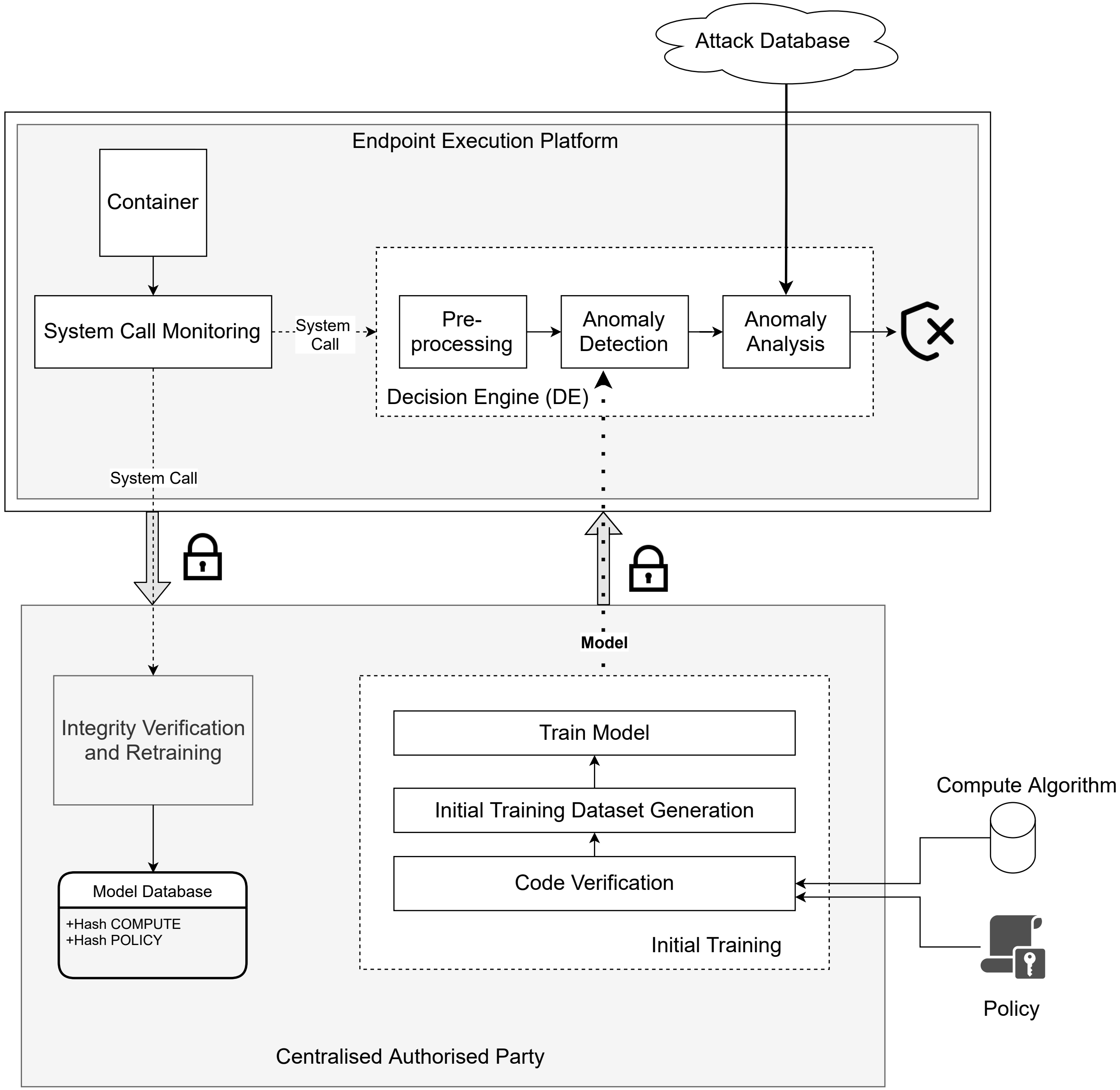
Profiling architecture

How to develop policy compliance detection components during execution?

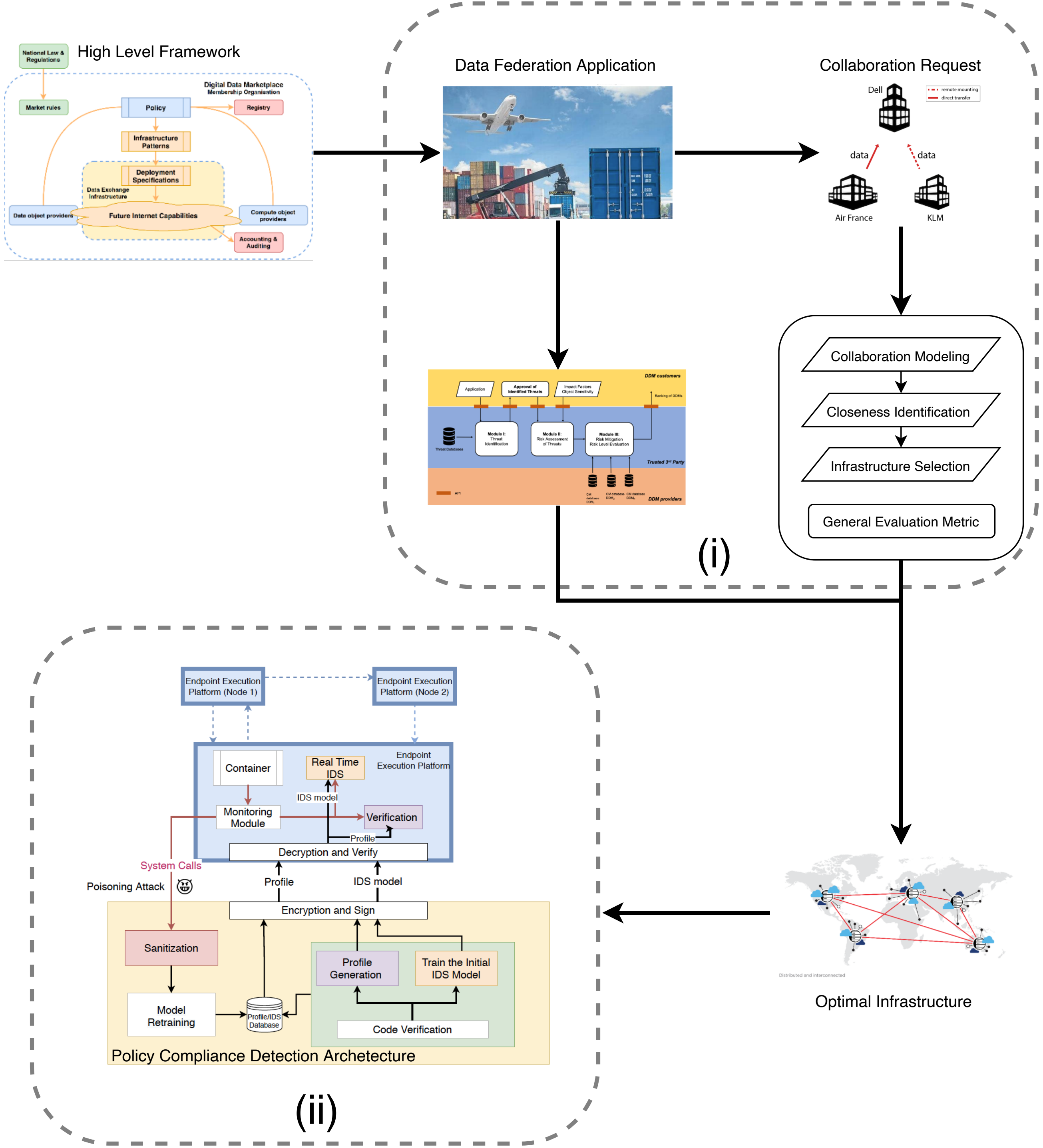




Intrusion detection



Architecture



A look at the future

Many interesting open venues for further research:

- extend the IDS to detect anomalies by monitoring multi-dimensional metrics.
  - Metrics related to the interactions between distributed execution platforms: traffic volumes and traffic patterns.
  - Metrics related to execution in a single execution platform: CPU or GPU usage, log information and memory access.
- combine different machine learning models and detect the anomalies in parallel
  - auto-encoder, generative adversarial networks, isolation forest, with different monitoring metrics.
- explore and expand the confidence area of a distributed IDS
  - investigate the possibility that a group of similar applications can share one pre-trained IDS model with sufficiently good detection performance.