Policy Enforcement for Secure and Trustworthy Data Sharing in Multi-domain Infrastructures

Xin Zhou
University of Amsterdam
Amsterdam, 1098XH
x.zhou@uva.nl

Reginald Cushing
University of Amsterdam
Amsterdam, 1098XH
r.s.cushing@uva.nl

Adam Belloum
University of Amsterdam
Amsterdam, 1098XH
a.s.z.belloum@uva.nl

Tom van Engers
University of Amsterdam
Amsterdam, 1098XH
T.M.vanEngers@uva.nl

Sander Klous
University of Amsterdam
Amsterdam, 1098XH
klous.sander@kpmg.nl

Cees de Laat
University of Amsterdam
Amsterdam, 1098XH
delaat@uva.nl

January 31, 2021

1 Abstract

The push for data sharing and data processing across organisational boundaries creates challenges at many levels of the software stack. Data sharing and processing rely on the participating parties agreeing on the permitted operations and expressing them into actionable contracts and policies. Converting these contracts and policies into an operational infrastructure is still a matter of research. In this paper, we investigate the architecture of a multi-domain distributed architecture for policy driven application. The architecture spans components from auditing policies to managing network connections.

The architecture is based on an auditable secure network overlays[3] proposed by Cushing et al. in 2020, the overlays have already introduced an audit layer and a control layer. The audit layer aims at checking if a certain data process is compliant, only those compliant ones can collect signatures, and forwarded to the control layer for further processing, such a mechanism ensures that all operations are audited before execution. This process is shown as fig 1: [1]

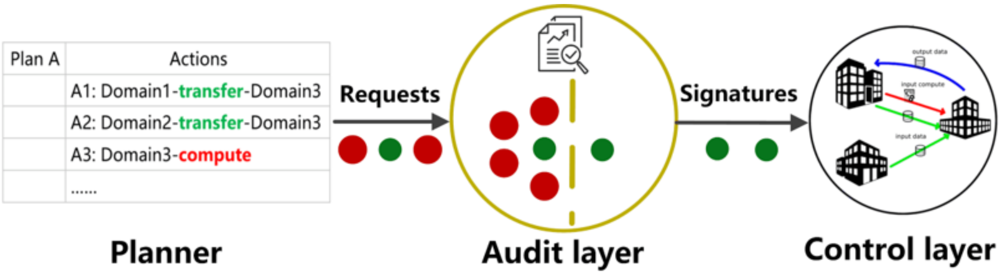

Figure 1: Auditable network overlays: the audit layer aims at checking the requests sent by a planner, only those compliant requests can receive signatures, and then being further executed in the control layer

To enforce the policies by the audit overlay, the unstructured or semi-structured policies expressed in natural language need to be structured and formalized first, before it can be used as input to the audit overlay and combined with the environment conditions (such as region, risk level, etc.) that clarify which policies should be applied. Fig 2 presents the conceptual view of the policy which contain authorisations, obligations, and environmental conditions [4, 2].

[1] This research is funded by the Dutch Science Foundation in Commit2Data program (grant no: 628.001.001).

Meanwhile, we introduced the concept of **manifest** which contains metadata of the dataset, the controller domain, the permitted recipients' domain, the corresponding applied policies, the sender domain, and a timestamp. This manifest is generated by the data controller or after a successful data transferring automatically. The manifest serves for the auditors to determine what policies they should comply with regard to a certain dataset. It also makes the data operation traceable as it is a record of when and where the dataset comes from.

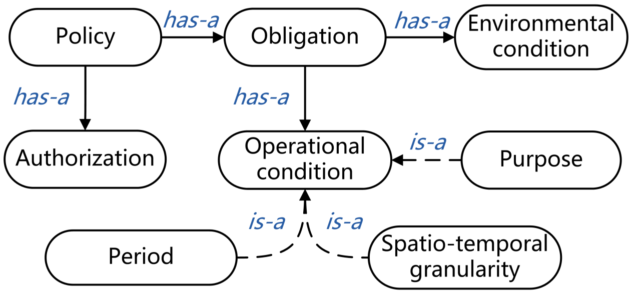

Figure 2: Conceptual view of the policy. It regulates the required auditors for the "Obligation" in "Authorisation". The "Obligation" can vary with "Environmental condition". Thus the latter is also specified in the policy. The clarification of purpose, period, and spatio-temporal granularity in the "Operational condition" defines the rights and duties in a fine-grained way.

We model the auditing process in Jason [1, 7], one of the most widely used development environments for a belief-desire-intention (BDI) [5, 6] based multi-agent system(MAS). Finally, we elaborate the proposed architecture by a realistic data-sharing use-case starting from policy down to the actual network connectivity.

Our proposed architecture and conceptual model guarantee the enforcement of data policies, essential for secure and trustworthy data sharing processes. Although our system aims at enforcing policies in a distributed infrastructure, it assumes all the policies are clear and conformant to higher order norms, such as legislation. However, in the real-world, policies like other sources of norms, including regulations, and laws, may contain expression with different levels of abstraction. The action/plan not only needs to be compliant with the concrete regulations, but should also in line with those abstract principles. How to enforce such hierarchical policies still needs further exploration. Also, in this work, we didn't consider a rectification mechanism. When the former executed actions contain uncertainty or indicate risks, then there should be options for rectifying. For example, if the obligation of self-identification was not fulfilled by the agent within the regulated time, which can cause some risks for its collaborators, then the infrastructure should be able to enforce the corresponding countermeasures like sending reminding to the agent, sending a warning to the collaborators, or even terminating the upcoming data processing related to that agent.

References

[1] Rafael H Bordini, Jomi Fred Hübner, and Michael Wooldridge. *Programming multi-agent systems in AgentSpeak using Jason*, volume 8. John Wiley & Sons, 2007.

[2] Quyet H. Cao, Madhusudan Giyyarpuram, Reza Farahbakhsh, and Noel Crespi. Policy-based usage control for a trustworthy data sharing platform in smart cities. *Future Generation Computer Systems*, 107:998 – 1010, 2020.

[3] Reginald Cushing, Ralph Koning, Lu Zhang, Cees de Laat, and Paola Grosso. Auditable secure network overlays for multi-domain distributed applications. In *2020 IFIP Networking Conference (Networking)*, pages 658–660. IEEE, 2020.

[4] Basel Katt, Xinwen Zhang, Ruth Breu, Michael Hafner, and Jean-Pierre Seifert. A general obligation model and continuity: enhanced policy enforcement engine for usage control. In *Proceedings of the 13th ACM symposium on Access control models and technologies*, pages 123–132, 2008.

[5] Zeshan Aslam Khan, Edison Pignaton de Freitas, Tony Larsson, and Haider Abbas. A multi-agent model for fire detection in coal mines using wireless sensor networks. In *2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, pages 1754–1761. IEEE, 2013.

[6] Inah Omoronyia. Reasoning with imprecise privacy preferences. In *Proceedings of the 2016 24th ACM SIGSOFT International Symposium on Foundations of Software Engineering*, pages 952–955, 2016.

[7] Giovanni Sileno, Alexander Boer, Tom M van Engers, et al. The institutional stance in agent-based simulations. In *ICAART (1)*, pages 255–261, 2013.