# Inverse Transparency for Cloud Architectures

Bachelor's Thesis


**Supervisor:** Prof. Dr. Alexander Pretschner
**Advisor:** Valentin Zieglmeier
**Email:** {pretschn, zieglmev}@in.tum.de
**Phone:** +49 (89) 289 - 17834
**Starting date:** immediately



Informatik 4 – Lehrstuhl für Software und Systems Engineering
Prof. Dr. Alexander Pretschner
Fakultät für Informatik
Technische Universität München

Boltzmannstraße 3
85748 Garching bei München

https://www.in.tum.de/i04/


## Context

To give employees more sovereignty over how their data are used, the concept of Inverse Transparency was introduced [1] (see also [2]). Access to data is therefore enabled on a more case-by-case basis, while monitoring all accesses and making each access visible to the data owner. This could allow individuals to trace usage of their data and hold data consumers accountable in case a data misusage is detected. The concept has been developed for company-internal infrastructures where control over data storing and consuming services lies with a single company. Yet, in many scenarios, services by third parties or intermediaries are used in practice (e.g. software-as-a-service), necessitating companies handing over their data and therefore losing oversight and control over it [3]. For such cloud applications, containers are increasingly used to ease deployment and orchestration [4]. Therefore, they serve as a relevant use case to focus on.

## Goal

This work considers the implications of these types of software deployments (SaaS / cloud) on Inverse Transparency. The topic is approached from two angles: (1) Broadly understanding the situation – how are cloud deployments implemented? and (2) tackling it with a concrete solution for containerized software. To that end, the work is split into three parts.

**Theoretical research:** The state of the art of cloud architectures is surveyed and compared with current and recent research. The field of cloud computing is developing quickly [5], necessitating an understanding of recent trends that are impactful for this research. In addition to a literature survey, real-world examples are collected. This should result in a taxonomy of cloud deployment variants and their implications for implementing Inverse Transparency.

**Implementation:** The existing Inverse Transparency toolchain [1] is extended for the concrete use case of Jira in the cloud. Specifically, an Inverse Transparency monitor for the Jira Docker container[1] will be implemented. The monitor should be pluggable into the container at deployment, e.g. via a docker-compose file. Its function will be to supervise traffic to Jira in the container and block invalid accesses, respectively log legitimate data usages.

**Evaluation:** Finally, the implementation is evaluated based on ease of deployment (how large are the necessary changes to the container), performance impact (compared to without monitoring), and its security (theoretical analysis of provided security guarantees).

## Work Plan

1. Survey academic literature and whitepapers from vendors on cloud architectures.
2. Create a taxonomy of cloud deployments and implications for Inverse Transparency.
3. Implement an Inverse Transparency monitor for the Jira Docker container.
4. Evaluate ease of deployment, performance impact, and deliberate security.
5. Document the work in the thesis.

## Deliverables

- Source code of the implementation.
- Thesis written in conformance with TUM guidelines.

## References


[1] Zieglmeier, Valentin, and Alexander Pretschner. "Trustworthy Transparency by Design." arXiv preprint 2103.10769 (2021). Available: https://arxiv.org/pdf/2103.10769


[1] https://hub.docker.com/r/atlassian/jira-software

[2] Barlow, Mike and Lévy-Bencheton, Cornelia. *The smart nation where everyone owns their personal data*. SmartCitiesWorld, 24th October 2018. Online: https://www.smartcitiesworld.net/special-reports/the-smart-nation-where-everyone-owns-their-personal-data

[3] Scaria, E., et al. "Study on data sharing between companies in Europe." A study prepared for the European Commission Directorate-General for Communications Networks, Content and Technology by everis (a NTT DATA company), 2018. Available: https://op.europa.eu/en/publication-detail/-/publication/8b8776ff-4834-11e8-be1d-01aa75ed71a1/language-en

[4] Pahl, Claus, et al. "Cloud container technologies: a state-of-the-art review." IEEE Transactions on Cloud Computing 7.3 (2017): 677-692. Available: https://www.researchgate.net/profile/Pooyan-Jamshidi/publication/316903410_Cloud_Container_Technologies_A_State-of-the-Art_Review/links/5a307e2aaca27271ec8a0bbc/Cloud-Container-Technologies-A-State-of-the-Art-Review.pdf

[5] Varghese, Blesson, and Rajkumar Buyya. "Next generation cloud computing: New trends and research directions." Future Generation Computer Systems 79 (2018): 849-861. Available: https://arxiv.org/pdf/1707.07452.pdf

Informatik 4 – Lehrstuhl für Software und Systems Engineering
Prof. Dr. Alexander Pretschner
Fakultät für Informatik
Technische Universität München

Boltzmannstraße 3
85748 Garching bei München

https://www.in.tum.de/i04/