Popular Science Summary

Why and how shared resources in the cloud can isolate users

Axel Sandqvist

Cloud systems share resources between many unaffiliated users, and to preserve confidentiality a compromise must be made between cost and isolation. How can resources be optimally utilised and also provide adequate isolation of users in a cloud system?

Shared resources for all users of a system, even those belonging to separate organisations- or tenants- can cause breaches in confidentiality if not handled with care. Improper authentication, authorisation or enforcement of policies set up by the system could cause data leaks and since the system is multi-tenant this could be to anyone in the system, not just within one organisation. To ensure tenant trust in the system, assurance of a stable system with decreased risk of data leaks especially between tenants but also within, is crucial. Essential mitigations for this are clear and concise demarcations between the tenants, my project answers how this is realised with reasonable assurance without significant costs.

The thesis' goal was to investigate the tenant separation of Axis Communication's platform ACX, which offers device management services. During analysis, room for improvement was found and a new design is proposed, suggesting increased clarity in enforcement of the separation between user data when querying databases, and a central access evaluation unit for increased maintainability and homogeneity for the otherwise diverse system.

Some interesting observations were found during the project. Increasing the separation within databases doesn't necessarily increase confidentiality, this is instead wholly dependent on how the data is fetched. Most technologies with greater separation between tenants shift the responsibility from the developers of the system to the infrastructure/the platform, where separate instances or entities are used to help keep data apart. This leads to increased costs since these divisions don't scale as well and requires additional resources. Another interesting observation is isolating processes(when data is updated in some way) is primarily used for systems with greater demands for privacy like healthcare or military systems. This means for the vast majority of systems on the internet, all data is processed with little to no isolation.

The results of this project are suggestions for change to the architecture of ACX, but may work as recommendations for similar large cloud services with many and varying functionalities. The main advantage of the improvements are increased isolation with the same resource utilisation and increased malleability of access control policies for efficiency and simplicity for the parties involved.

Storing and processing data in the cloud is a great opportunity because of the relatively cheap services, ease of use and possibilities of geographical distribution. The trend of most software systems today is to migrate to the cloud, however these benefits of the cloud come with new obstacles to overcome. My report provides support in choosing which separation technology to apply and what to consider when planning the multitenant architecture.