A secure network overlay for tracking and enforcement of data transaction rules.

Ralph Koning, Reginald Cushing Lu Zhang, Cees de Laat, Paola Grosso, University of Amsterdam

Competing companies can, together, generate value from collaborating on data and compute. Examples include airlines industry, ports, healthcare. Clearly this poses a challenge of how to facilitate such collaborations through technology. Here we look at one piece of the puzzle i.e. setting up distributed multi-domain infrastructures between such parties to facilitate the running of applications.

**Overlay**
- Nodes on the network are addressed using their public key.
-Nodes include: domain controllers, data buckets, auditors, application planners, users.
- Keys create chains of trust and verification through cryptographic signature trails.
- Applications are decomposed to a set of transactions.
- Transactions drive the overlay.

**Network of Auditors**
- Auditor nodes on the network provide a signing and verification layer that is checked by the control layer.
- Auditors sign network actions based on their internal policy.
- Auditors are independent of each other.
- The more number of signatures an action gets (e.g. transaction) the more confident the control layer is.
- Auditors cross-verify each other’s logs to minimize log tempering.

**Motivation**
- Multi-domain distributed applications need to share data and compute under different policies.

**Challenges**
- Map data sharing policies to infrastructure.
- Build an infrastructure that facilitates these applications.
- Control sharing of data and compute.
- Audit activity of the network.
- Minimize risk of policy/security breaches.

**Control functions**
- Securing bucket-to-bucket communication through transaction specific VPNs.
- Bucket node key address used as VPN keys.
- Opening connection endpoints on audit signatures.
- Network interfaces created on demand. Bucket containers have no network interface. Interfaces are only created and attached per signed transaction.

In short...
- Overlay allows for a distributed infrastructure.
- Key-based addressing allows for node signature trails and trust chains.
- Network of auditors provide rubber-stamping of actions/transactions
- Control layer enforces security using inputs from auditors and minimizes attack vectors on data transfers.

Proof of Concept, see [https://dl4ld.nl/](https://dl4ld.nl/)

This research is funded by the Dutch Science Foundation in the Commit2Data program (grant no: 628.001.001) and by Equinix.