imec

An imec.icon research project | project results

ICT

Middleware for scalable, attribute-based querying of multitenant, cloud-based databases

There is a growing trend to subscribe to software services in the cloud. An example is a large corporation that creates, views, and manages massive amounts of invoices in the cloud through a SaaS service (Software as a Service). However, in general such services don't offer many possibilities to restrict queries based on e.g. security or privacy considerations. And without such restrictions, an individual account manager, for example, can query and see all the invoices, irrespective of his role, assigned customers, or region. In addition, the SaaS provider cannot easily make its database multitenant, i.e. shared by a number of its customers.

A common way to solve this problem today is for the SaaS providers to set up separate installations per customer and to program the security logic in the application, a solution that is most often not efficient, error-prone, difficult to audit and expensive to adapt.

With SEQUOIA, we aimed to develop a generic solution for SaaS providers. A solution that allows them to set up one multitenant database while giving each of their customers the possibility to define fine-grained, attribute-based security rules. In the invoice example, the corporation using SaaS would then be able to set restrictions on viewing and modifying invoices based on e.g. region, responsibility, or account management.

Koen Handekyn, project lead and CEO of UP-nxt, says: "The solution we came up with is a real innovation compared to the state-of-the-art. In essence, it replaces the manual process where software developers of the SaaS provider have to program authorization into the queries. This has proven error-prone and is very difficult to audit by the customers. With SEQUOIA, the SaaS customers can now add their own authorization rules, in a declarative language that is easy to use and to audit. With these rules, the queries are then automatically tailored before they are executed, instead of having the application filter the results after a database search. This rewriting and compacting of queries is done by an add-on module, at the level of the data access middleware, and is thus separated from the database or customer applications. This allows SaaS providers like us to add value to their service without having to install new databases or middleware, or reprogram the applications."

THE OUTCOMES

1. **A security solution to enforce complex, custom authorization rules in search queries, with guarantees for safety, correctness and performance**

SEQUOIA offers a language to create a declarative access rule base based on attributes. This guarantees independence for application code, easy access, modification and audit. Because the rules are applied before querying, the performance does not relate to the size of the database.

2. **Security middleware for SaaS, generic and application-independent**

SEQUOIA is implemented as an add-on to the data access middleware, the API that sits between a database and the query source (customer application, web server...). The solution takes in a query, looks up the relevant security rules, translates these into restrictions that it injects into the query, and then compacts the query before it is sent on to the database. It can be added to proven, state-of-the-art data access middleware without having to rebuild a solution from scratch.

3. **Validated in multiple storage and query architectures, with proof-of-concept in state-of-the-art data access middleware**

SEQUOIA's solution was validated for interactive and background querying, both with SQL structured queries and NoSQL unstructured querying.

4. **Demonstrators in the three application domains of the partners**

Active in three non-overlapping domains, SEQUOIA's partners cover a variety of possible use cases for SaaS querying. UP-nxt manages customer administration data such as invoices, which have access ruled down to the level of single account managers, regions... Verizon has multitenant databases containing logs of managed IT infrastructure, access to which is extremely sensitive and restricted. And ESAS wants to set up a field service management where service engineers in the field can access their tasks, messages and statuses.

NEXT STEPS

The three companies that participated in SEQUOIA now have the expertise and software to enhance their SaaS offering. They may work towards validating and including the new middleware into their live environments, which will offer them three competitive advantages:

- Mitigate the lingering doubt of customers about the security of multitenant cloud solutions. With the SEQUOIA solution, each customer will own, validate and audit its own rule base.
- Adding value for the customers (which translates into business value for the SaaS provider), mainly because of the unique possibility to set up customer-specific rule bases.
- Lowering operating cost, as SEQUOIA allows for one multitenant cloud installation, with no need for dedicated installations per business case.

AGENTSCHAP INNOVEREN & ONDERNEMEN
Vlaanderen is ondernemen
The SEQUOIA project was co-funded by imec (iMinds), with project support from Agentschap Innoveren & Ondernemen.

FACTS

NAME	SEQUOIA (Safe Query Applications for Cloud-Based SaaS Applications)
OBJECTIVE	Create a security framework for advanced queries and reporting in large, multitenant SaaS environments, allowing the efficient application of fine-grained security rules following each tenant's business logic
TECHNOLOGIES USED	Both SQL and NoSQL technologies (e.g. SQL server, Elastic Search, Hadoop) as well as data access middleware (e.g. JPA)
TYPE	imec.icon project
DURATION	01/01/2015 – 31/12/2016
PROJECT LEAD	Koen Handekyn, UP-nxt
RESEARCH LEAD	Wouter Joosen, imec - DistriNet - KU Leuven
BUDGET	2.455.725 euro
PROJECT PARTNERS	ESAS, Verizon, UP-nxt
IMEC RESEARCH GROUPS	DistriNet - KU Leuven, IDLab - UGent

WHAT IS AN

IMEC.ICON PROJECT?

The imec.icon research program equals demand-driven, cooperative research. The driving force behind imec.icon projects are multidisciplinary teams of imec researchers, industry partners and / or social-profit organizations. Together, they lay the foundation of digital solutions which find their way into the product portfolios of the participating partners.

SEQUOIA project partners:

esas verizon UnifiedPost

AMERICAS
raffaella.borzi@imec.be
T +1 408 386 8357

CHINA
timo.dong@imec-cn.cn
+86 13564515130

EUROPE & ISRAEL
michel.windal@imec.be
+32 478 96 67 29

JAPAN
isao.kawata@imec.be
T +81 90 9367 8463

TAIWAN & SE-ASIA
mavis.ho@imec.be
T +886 989 837 678

VIETNAM, BRAZIL, RUSSIA, MID EAST, INDIA
max.mirgoli@imec.be
T +1 415 480 4519