imec

An imec.icon research project | project results

ICT

SeClosed

Secure, Cloud-based Storage and Processing of Sensitive Documents

Companies and organizations more and more rely on software services that are implemented in the cloud, the so-called SaaS services (Software as a Service). Examples are telecom operators that create and manage massive amounts of invoices, or hospitals that manage patient records. They take out a subscription with a SaaS provider to have their data managed and stored.

There is, however, a mounting security and privacy concern. Customers rely on SaaS providers to keep their sensitive documents – invoices, patient records – secure and private. But these SaaS providers in their turn will subscribe to data centers and storage solutions that may be outside of their control, services offered e.g. by Microsoft or Amazon and physically located on the other side of the globe.

This calls for additional trust barriers between the SaaS provider, storage solutions and hosting providers. These should be trust barriers where the control and keys are in the hands of the trusted SaaS providers and where the sensitive documents remain opaque at all times for the storage and hosting providers.

“With SeClosed, our goal was to develop the basis for a generic security solution for SaaS providers,” says Koen Handekyn, project lead and CEO of UP-nxt at the time. “We did this in the form of a customizable add-on to existing and widely-used data access middleware, an add-on that gives application developers a powerful access to advanced encryption strategies and that takes away the burden to implement and integrate these on their own.”

The solution that the SeClosed partners envisioned allows to annotate data elements separately as a way to indicate their security requirements and to define policies concerning where and how these elements should be stored and which encryption tactics should be used. “That encryption could be a standard scheme (such as AES), but then the documents cannot be searched without first retrieving and decrypting them,” says Wouter Joosen, director of DistriNet, an imec research group at KU Leuven. “More intelligent data protection tactics allow searching in encrypted data, or applying functions on encrypted data. The latter tactics include homomorphic encryption. They largely belong to the domain of research. In this project, however, we have examined how we could apply them to two practical use cases.”

The two research partners are top in their field: DistriNet has an extensive expertise in the design and implementation of data access middleware, and COSIC is famous for its research on encryption tactics. UP-nxt and Agfa Healthcare are two SaaS providers looking to extend their expertise, and Proximus is a trusted storage and hosting provider.

THE OUTCOMES

1. Add-on to existing data-access middleware

SeClosed has developed an add-on to existing, widely-used data access middleware for secure multi-cloud storage (e.g. Hibernate). This solves the issue of SaaS application developers who are often unable to deal with complex cryptographic API calls in application code.

The add-on is easily configurable. It is annotation- and policy-driven and allows defining rules and appropriate storage and encryption tactics per data element. That way, it is for example possible to define which elements can be stored locally and unencrypted with a trusted intermediary, and which elements should be stored in the cloud and remain encrypted at all times.

2. Implementing both real-time and background analysis on encrypted data

SeClosed developed two types of advanced application-specific encryption tactics. One is for text-based search with full encryption of the index and database, and the second involves homomorphic encryption tactics for sums and averages. These were developed for use on top of unchanged NoSQL databases such as Cassandra, MongoDB or ElasticSearch. These solve the key issue that current operations and data aggregation functions cannot be applied to encrypted data in the storage environment.

3. Validation in the application domains of two partners

UP-nxt offers SaaS services to manage financial data and documents such as invoices. Once these have been encrypted and stored, UP-nxt's customers may want to query for all open invoices of an organization, or for totals of invoices. In SeClosed, we made a number of schemas that allow doing these queries on the encrypted data.

Agfa Healthcare managed medical documents and patient records for e.g. hospitals. The challenge is to allow datamining without first decrypting all the data. One example that we developed is computing the average BMI (Body Mass Index) for all people from a region or city. To do so, we had to carefully examine what was possible with homomorphic computing to arrive at a practical solution.

NEXT STEPS

The companies that participated in SeClosed have increased their know-how and expertise to improve their SaaS offering and the trust of their customers. They now have additional arguments and potential instruments to mitigate the lingering doubt of customers about the security of cloud solutions. For UP-nxt and Agfa Healthcare, that has translated in a SaaS solution validation that may form a basis for further work.

For both research groups, this project has also allowed building valuable expertise with real-life use cases. For DistriNet, this translates in additional building blocks in their security-enhancing middleware R&D track; for COSIC, there is now a basis to match real-life database querying to the most advanced encryption strategies, helping the researchers to remain top in the field.

In general, this project has advanced a field that is becoming more and more important and in which many Flemish ICT actors are active.

AGENTSCHAP INNOVEREN & ONDERNEMEN
Vlaanderen is ondernemen

The SeClosed project was co-funded by imec (iMinds), with project support from Agentschap Innoveren & Ondernemen.

FACTS

NAME	SeClosed (Secure, Cloud-based Storage and Processing of Sensitive Documents)
OBJECTIVE	The SeClosed project aims to deliver a set of data protection techniques and data access middleware for secure document storage and processing. These solutions can be deployed in cloud environments and other untrusted storage solutions.
TECHNOLOGIES USED	Both SQL and NoSQL technologies (e.g. SQL server, Elastic Search, Cassandra) as well as data access middleware (e.g. Hibernate, JPA)
TYPE	imec.icon project
DURATION	01/04/2016 – 31/03/2018
PROJECT LEAD	Koen Handekyn, UP-nxt
RESEARCH LEAD	Wouter Joosen, DistriNet
BUDGET	1,911,151.21 euro
PROJECT PARTNERS	Agfa Healthcare, Proximus, UP-nxt
IMEC RESEARCH GROUPS	DistriNet & COSIC, imec research groups at KU Leuven

SeClosed project partners:

AGFA HealthCare · proximus · UP nxt

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.

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

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

EUROPE & ISRAEL
michel.windal@imec.be
T +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

DISCLAIMER - This information is provided 'AS IS', without any representation or warranty. Imec is a registered trademark for the activities of IMEC International (a legal entity set up under Belgian law as a "stichting van openbaar nut"), imec Belgium (IMEC vzw supported by the Flemish Government), imec the Netherlands (Stichting IMEC Nederland, part of Holst Centre which is supported by the Dutch Government), imec Taiwan (IMEC Taiwan Co.) and imec China (IMEC Microelectronics (Shanghai) Co. Ltd.) and imec India (Imec India Private Limited), imec Florida (IMEC USA nanoelectronics design center).