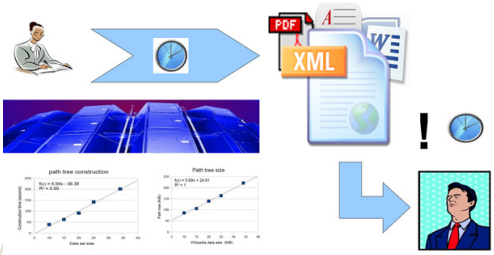
EFFICIENT QUERYABLE ENCRYPTION SOLUTION FOR DOCUMENTARY DATABASE

Storage and querying of documentary database in the cloud while ensuring end-to-end content confidentiality with minimum time and memory resources.

ERGANEO
L'AVENIR EST FAIT D'AUDACE

PRESENTATION

Homomorphic cryptography makes it possible to host encrypted documents in the Cloud, while offering queries on their content, without exposing secret data. However, many Internet applications of document computing require processing massive streams of XML data, which poses real technological challenges for the efficiency of processing techniques and data security. CSQM, the completely new model proposed, is a flow processing approach which makes it possible to minimize the consumption of resources (time, memory) for a given request on a document of any size.



Queryable encryption - Structured encryption
Confidential cyphered Stream-Querying Model (CSQM)
XML data and XPath queries

APPLICATIONS

- Queries on secret data in the cloud, such as personal or medical, with guarantee of privacy and confidentiality
- Allow a safe collaboration with external or third parties on encrypted secure data stored in the cloud, without exposing the underlining data.
- Query system on end-to-end encrypted messaging systems. Queryable archive of confidential messaging mailboxes.

COMPETITIVE ADVANTAGES

- Minimum consumption of resources (time, memory) for a given request on an encrypted document of any size
- Resistance to active sub-document injection attacks (structure integrity)
- Interactive model between the end user and the system in order to automate and optimize the processing of requests according to the user's needs
- Overheads for encryption are predictable and linear in time and space

DEVELOPMENT PHASE

- ☑ Executable code of the different modules of CSQM available for testing purpose

INTELLECTUAL PROPERTY

Deposit of the software at the APP under number IDDN.FR.001.150002.D. P.2012.000.20800

PUBLICATIONS

Alrammal, Muath, and Gaétan Hains. «Forward XPath stream processing: End-to-end confidentiality and scalability.» *2014 10th International Conference on Innovations in Information Technology (IIT)*. IEEE, 2014.

Alenezi, Mamdouh & Usama, Muhammad & Almustafa, Khaled & Iqbal, Waheed & Raza, Muhammad & Khan, Tanveer. (2019). An Efficient, Secure, and Queryable Encryption for NoSQL-Based Databases Hosted on Untrusted Cloud Environments. International Journal of Information Security and Privacy. 13. 14-31. 10.4018/IJISP.2019040102.

CONTACT

+33 (0)1 44 23 21 50
industriels@erganeo.com
Ref. project : 313