PARSEC.CLOUD : Secure File Storage and Sharing

Stefan Contiu, Emmanuel Leblond, François Rossigneux, Maxime Grandcolas, Nicolas Stempert,
Vincent Michel, Thierry Leblond, Philippe Clermont and Laurent Reveillere*
Scille SAS, *University of Bordeaux, France - stefan.contiu@scille.fr

***Abstract*—We describe the PARSEC.CLOUD project, developed by SCILLE and financed by DGA RAPID-172906010 between Feb. 2017 and Feb. 2019.**

I. INTRODUCTION

Public cloud storage services represent an efficient alternative to private (e.g. *in-house*) storage infrastructures. They offload the complexity of setting up, maintaining and scaling the infrastructure from the hands of end clients. Moreover, attractive subscription plans require paying only consumed resources (e.g space or bandwidth). Nevertheless, cloud storage comes with a high security risk. Numerous incidents report malicious users bypassing the provider security protocols and gaining access to sensitive user data. Also, hosted data can be warranted by governments for national interest (e.g. *Cloud Act* in *US*). As such, public cloud providers fail to offer strong security guarantees to end users with respect to the entrusted data.

PARSEC.CLOUD is an open source [1] software solution designed to addresses the security concern of public cloud services while leveraging their advantages (e.g. scalability, pay-per-use). PARSEC.CLOUD cryptographically protects the user data on the client side, enforcing exclusive possession of cryptographic keys solely by the clients. In addition, PARSEC.CLOUD guarantees the data integrity, authenticity, traceability, and a high level of availability.

II. PARSEC.CLOUD SOFTWARE PRODUCT

The development of PARSEC.CLOUD followed a four milestones plan, each reviewed and signed-off by DGA. If the first one required the delivery of exhaustive functional, design and *state-of-the-art* specifications, the subsequent three milestones required the delivery of incremental system functionalities. At the time of writing, PARSEC.CLOUD reached the final implementation stage of v.1. (*Community Edition*), currently in *beta testing* with an estimated commercialization starting in the second quarter of 2019. An upcoming v.2. (*Enterprise Edition*) is scheduled to integrate the outputs of our research activity (see Section III).

In a nutshell, the architecture of Parsec employs a three layer separation : the client application, the metadata service and the cloud storage providers. Files are broken into symmetrically encrypted blocks while metadata of user files and composing blocks are protected by the user private key. The encrypted blocks are redundantly stored over multiple cloud storages. Users are able to synchronize files among multiple devices or with a group of fellow users. The design is crash tolerant and optimizes the user experience.

[1]https://github.com/Scille/parsec-cloud

III. RESEARCH WORK

The research activity, complementary to the product development work, focused on finding potential risks and addressed design and development challenges.

We identified a lack of comprehensive comparison of the costs and effectiveness of cryptographic primitives for securing public cloud storage. We performed a benchmarking study [1] which emphasizes that the choice of a cryptographic scheme is highly dependent of the target usage conditions. As such, we provide a set of selection guidelines per undergoing cloud specific workloads.

We investigated the efficiency of *state-of-the-art* cryptographic access control mechanisms [2]. Preliminary benchmarking showed unsatisfiable performance of existing methods when considering large and dynamic membership conditions. We proposed a novel cryptographic construction IBBE-SGX [3] leveraging Identity Based Broadcast Encryption in conjunction with Trusted Execution Environments, concretely Intel SGX. IBBE-SGX is 1.2 orders of magnitude (OoM) faster and produces 6 OoM less metadata than the traditional approach of *hybrid encryption*.

A particular interest was given to *state-of-the-art* revocation capabilities, which are either secure but slow (e.g. *active revocation*) or fast but not entirely secure (e.g. *lazy revocation*). We proposed a *hybrid revocation* mechanism [4] that can achieve high security guarantees with practical performance. Our scheme makes use of All or Nothing Transform (AONT) coupled with Intel SGX, and is 3 order of magnitude faster than *active revocation* technique.

Current and future research lines explore the *anonymity* of group access control, and decentralized access control through *blockchain*-like technology.

The research work is performed in joint collaboration with University of Neuchâtel (*CH*) and Universitè catholique de Louvain (*BE*).

IV. CONCLUSION

We have presented PARSEC.CLOUD : a client side enforced secure cloud storage and sharing solution. We justified the context, and provided key product development and research aspects.

REFERENCES

[1] S. Contiu, E. Leblond, and L. Réveillère, "Benchmarking cryptographic schemes for securing public cloud storages," in *DAIS*, 2017.
[2] S. Contiu, "Towards efficient cryptographic group access control systems," in *EUROSYS Doctoral Workshop*, 2018.
[3] S. Contiu, R. Pires, S. Vaucher, M. Pasin, P. Felber, and L. Réveillère, "Ibbe-sgx: Cryptographic group access control using trusted execution environments," in *DSN*, 2018.
[4] S. Contiu, L. Réveillère, and E. Rivière, "Hybrid revocation using trusted execution environments," in *Compass*, 2018.