Protection of data in cloud computing including distributed environments is a critical concern for many enterprises. This study proposes a solution that protects sensitive data outsourced to a cloud throughout their entire life cycle—both in the cloud as well as outside of the cloud (e.g., during transmission to or from the cloud). The solution enhances the existing data protection approach known as Active Bundle scheme, which uses a Trusted Third Party (ABTTP).

The Active Data Bundle (ADB) was formerly called an Active Bundle (AB). It is a software construct that encapsulates data, metadata, and a virtual machine (VM). The metadata includes, among other aspects, data access and data privacy policies for the ADB’s data. The VM executes and directs ADB active operations on its sensitive data and metadata, such as enforcement of
all ADB policies (included in metadata), integrity self-checking, evaporation (that is, a partial ADB self-destruction), and apoptosis (that is, a complete ADB self-destruction). The current ADB implementation relies on a centralized trusted third party (TTP) server. Using a centralized TTP in ABTTP increases the risks of many attacks, including side channel and correlation attacks.

Our solution, known as Active Data Bundle using Secure Multiparty Computation (ADB-SMC), uses: (i) active data bundles (ADBs) for self-protecting data; (ii) ciphertext-policy attribute-based encryption for fine-grained access control; (iii) threshold RSA to eliminate the problem posed by centralized TTPs; and (iv) multi-agent systems (MAS) to reduce network traffic and support fault tolerance. We have implemented a prototype of ADB-SMC on five hosts and re-implemented the prototype of ABTTP to record measurements and compare the overhead of the two solutions. The results of performance tests on our ADB-SMC prototype show that the execution time overhead is acceptable.

The features that distinguish ADB-SMC comparing to previous ABTTP solutions are: (i) improvement of the creation, dissemination, and trust management of the earlier implementations; (ii) providing higher security and fault tolerance due to eliminating an easy target in the form of a single centralized TTP for key management; (iii) implementing a data access policy to support secure fine-grained access control for ADB data; (iv) protecting against data loss and reducing ADB dissemination overhead in the cloud by using secure ADB backup services; and (v) deploying the solution on multiple hosts using an inter-platform mobility service (IPMS). IPMS is suitable for a distributed environment since it uses a "one-shot" migration strategy to transfer data and code every time an agent moves, thus supporting fault-tolerance.

Our solution has a significant impact on protecting privacy in clouds and many other distributed systems. The effects are noticeable for an application having, among others, the following needs: (i) full protection of privacy of sensitive data throughout their entire lifecycle; (ii) full protection of privacy of sensitive output data on untrusted hosts; (iii) strong data and IDM (identity management) security in clouds and other distributed computing systems; (iv) fault tolerance; and (v) efficiency due to exploiting parallelism.