Забезпечення інформаційної безпеки в хмарних сховищах даних

Бєлоус Д.І., *студ.*; Кучернюк П.В., *доц.*
Національний технічний університет України
«Київський політехнічний університет», м. Київ

З розвиненням інфраструктури, підвищенням доступності й швидкості інтернету, а з іншого боку із збільшенням кількості даних у користувачів комп'ютерів та мобільних пристроїв все більшої популярності набувають хмарні сховища даних. В дослідженнях [1] неодноразово показано слабкі місця з боку забезпечення цілісності та конфіденційності даних в існуючих рішеннях. Найчастіше в наявних сервісах можна виділити наступні проблеми: відсутнє шифрування даних користувача взагалі; шифрування даних на стороні сервера, а отже власник хмари має усі ключі і за потреби надасть їх третій стороні; відсутність захисту цілісності даних. Такі умови використання не підходять для підприємств і державних організацій.

Метою роботи було створення ефективного захищеного рішення, яке працює на стороні клієнта і забезпечує конфіденційність й цілісність даних користувача в хмарному сховищі. При переносі усіх операцій захисту інформації зі сторони сервера на сторону клієнта, користувач не зобов'язаний довіряти відповідальність за конфіденційність його даних хмарному сервісу. В основу рішення було покладено використання метода криптографічного контролю доступу [2] та систему розподіленого файлового сховища Infinispan. Криптографічний контроль доступу передбачає шифрування даних на стороні клієнта за допомогою симетричного алгоритму шифрування, їх підпис приватним ключем за допомогою асиметричного алгоритму шифрування та перевірка, перед записом/обновленням файлу на стороні серверу, підпису користувача за допомогою публічної частини ключа. Таким чином, забезпечуються конфіденційність та цілісність даних. В роботі проаналізовано отримане рішення та проведено оцінку його ефективності, швидкодії та захищеності. Отримане рішення може бути використано для створення хмарного сховища, для клієнтів якого конфіденційність та цілісність даних є критичним фактором.

1. M. Dam, K. Chen, On the Security of Cloud Storage Services (2013).
2. A. Harrington, C.D. Jensen, *SACMAT* **03**, 158 (2003).