УДК 004.056.55

ВИКОРИСТАННЯ ГІБРИДНОЇ КРИПТОГРАФІЇ В «ХМАРНИХ» ТЕХНОЛОГІЯХ КОМП’ЮТЕРНИХ ОБЧИСЛЕНЬ

Квєтний Роман, Титарчук Євгеній

Вінницький національний технічний університет

Анотація

Запропоновано новий підхід та створену на основі нього програму для захисту інформації користувача при роботі з хмарним сервісом збереження файлів DropBox. Данна програма шифрує файли перед їх відправленням у хмару та дозволяє отримувати доступ до файлів визначеній групі користувачі.

Abstract

The new approach and based on it program for the protection of user files when working with cloud service for file storing DropBox is introduced. This program encrypts files before sending them to the cloud and lets you access files specific group of users.

Вступ

Останнім часом хмарні технології набули надзвичайно широкого розповсюдження. Вони використовуються для синхронізації даних, розподілених обчислень, збереження та передачі файлів, тощо.

Під час використання хмарних обчислень програмне забезпечення надається користувачеві як Інтернет-сервіс. Таким чином «хмара» це такий спосіб комп’ютерних обчислень при якому данні користувача постійно зберігаються на серверах хмарного сервісу і хоча користувач має доступ до власної інформації в хмарі, але зазвичай не може управляти її інфраструктурою.

В цьому проявляється головний недолік хмари – приватна інформація користувача фактично стає доступна третій стороні – провайдеру, крім цього данні можуть стати вразливими під час їх передачі по каналам зв'язку [1].

Актуальність

Актуальність даної роботи полягає у необхідності збереження персональних даних користувача та недоліками існуючих на ринку програмних продуктів які призначених для захисту інформації від її доступу третій стороні при використанні хмарних рішень збереження даних.

Метою даної роботи є покращення ефективності захисту файлів користувача з можливістю надання доступу до них певній групі осіб, при використанні хмарного сервісу збереження файлів DropBox на основі аналізу існуючих хмарних рішень та моделі їх представлення користувачам.

Задачі

1. Дослідити наявні небезпеки приватній інформації при використанні хмарних рішень збереження даних.
2. Розробити математичне, алгоритмічне та програмне забезпечення для захисту файлів користувача при використанні хмарного сервісу DropBox.
3. Розробити алгоритмічний апарат для надання можливості користувачам спільного використання зашифрованих файлів.

Гібридне шифрування при використанні хмарного сервісу

Нехай користувач має логін (L) та пароль (P). Для шифрування файлів користувача використаємо еліптичну криву $E_p(a,b)$. За допомогою хеш функції $H(x)$ з літеро-цифрового паролю P довільної довжини отримуємо закритий ключ n_A визначеної довжини.

$$n_A = H(P)$$

При реєстрації на основі паролю n_B та точки G, що належить даній кривій генерується відкритий ключ P_B та ставиться у відповідність логіну L

$$P_A = n_A \times G$$
$$L \sim P_A$$

тоді ми можемо використовувати логін як відкритий ключ. Після цього для шифрування визначається секретний ключ К

$$K = n_A \times P_A$$

Секретний ключ К можна використати у якості сеансового для алгоритму симетричного шифрування (AES). Логін (фактично публічний ключ) прикріпляється до файлу.

При необхідності дати можливість доступу до певного файлу відразу декільком користувачам секретний ключ матиме наступний вигляд:

$$K = n_0 \times P_i \times \ldots \times P_n ,$$

де n_0 – закритий ключ користувача що шифрує файл,
$P_{i\ldots n}$ – відкриті ключі користувачів яким необхідно надати доступ до файлу.

Кожному окремому користувачу повинні бути відомі логіни інших.

Розробка програмного забезпечення

Головна функція даної системи – синхронізація однієї з папок комп'ютера користувача з його обліковим записом у хмарному сервісі DropBox. Система використовує гібридне шифрування, що поєднує еліптичну криптографію для обміну ключами та симетричний шифр AES для шифрування файлів. Під час синхронізації файли розшифровуються та зашифровуються на клієнтському комп'ютері, таким чином на сервісі зберігаються тільки зашифровані версії файлів користувача. Використання асиметричного шифру дає можливість створювати файли які можуть розшифрувати декілька користувачів.

Висновки

Після аналізу загроз безпеці приватної інформації зроблено висновок що використання гібридного шифрування приватної інформації користувача при збереженні її в хмарному сервісі дозволить зробити її недоступною для третьої стороні в більшості з перерахованих[1] сценаріїв, а також дозволить використати сервіс для пересилки файлу іншим особам. На основі цього розроблено програму CryptoBox що шифрує дані на стороні клієнта, перед відправленням на хмарний сервіс, за допомогою стійкого симетричного алгоритму шифрування, також розглянуто існуючі аналоги створеної системи.

Список використаних джерел:

1. Захист даних в хмарних технологіях обчислень [Електронний ресурс]: Захист даних в хмарних технологіях обчислень // ВНТУ – ВНТУ. – Режим доступу: http://conf.vntu.edu.ua/allvntu/2013/inaeksu/txt/tytarchuk.pdf. – Назва з екрану.

2. Peter Mell, Timothy Grance. The NIST Definition of Cloud Computing / National Institute of Standards and Technology / Rebecca M. Blank. – Gaithersburg: NIST, 2011. – 286 с.

3. Google Engineer Spied on Chats [Електронний ресурс] / Gawker. – Режим доступу: http://gawker.com/5637234/gcreep-google-engineer-stalked-teens-spied-on-chats

4. Dropbox Core API [Електронний ресурс]: Dropbox Core API // Dropbox – Dropbox. – Режим доступу: https://www.dropbox.com/developers/core/. – Назва з екрану.