УДК 004.75:004.05

І.Д. ГОРБЕНКО, д-р техн. наук, М.І. ХАРЛАМБ

МЕХАНІЗМИ ЗАХИЩЕНОГО ОБМІНУ ІНФОРМАЦІЄЮ ПРИ ВИКОРИСТАННІ ХМАРНИХ ОБЧИСЛЕНЬ

Вступ

Технологія хмарних обчислень на даний момент розвивається дуже потужно, особливо у сфері обробки великого об'єму інформації. Разом з цим використання хмарних обчислень[1] не тільки дозволяє реалізувати можливість віддаленої обробки інформації та забезпечує досягнення високих показників відмовостійкості інформаційної інфраструктури, але й вносить додаткові загрози інформаційній системі та особисто інформації, що там обробляється.

Необхідності забезпечувати певний рівень захисту даних сприяють деякі властивості системи хмарних обчислень, які з одного боку роблять технологію рентабельною та актуальною, а з іншого надають зловмиснику можливість посягання на сторонні конфіденційні дані. Якщо головним для користувача є забезпечення конфіденційності при обчисленнях в хмарах, то найкращим засобом захисту можна назвати криптографічний захист інформації. Таким чином, для розробки системи захисту інформації будуть застосовуватися певні шифри, протоколи захищеного обміну даними, направлене шифрування та інші засоби криптографічного захисту. Серед наведених засобів забезпечення конфіденційності оброблюваної інформації найбільш достовірними та поширеними вважаються протоколи захищеного обміну даними.

В даній роботі зроблено докладний опис обраного механізму, проведено його аналіз та рекомендації щодо застосування в реальних системах. Актуальність розгляду питання підтверджується попередніми роботами з цієї тематики [1, 3, 4], а також зручністю та надійністю використання механізмів захищеного обміну даними, як на стороні клієнтської частини програмного комплексу, так і на відповідній програмній частині серверу. Актуальність вивчення таких механізмів можна також обгрунтувати зацікавленістю й постійною роботою з удосконалення технологій у цьому напрямку багатьох світових корпорацій, які розробляють власні програмні компоненти та здійснюють їх впровадження на різних рівнях: SunMicrosystems, RSASecurity, Netscape.

Спрощене подання системи хмари

Для того щоб детально зрозуміти, як працює той чи інший протокол обміну даними у хмарі, треба мати уяву, як він взаємодіє із компонентами хмари та її функціональними частинами. З цією метою треба скласти спрощену структуру хмари та створити модель маршрутів інформації в системі, тобто описати процес взаємодії даних в хмарі. Спрощена модель хмари представлена на рис.1.

На рисунку під хмарою розуміється спрощене подання сукупності технологій та апаратного забезпечення, що складається із обчислювальних ресурсів, сховищ даних, апаратури віртуалізації, сервера управління запитами і так далі. Адмініструючий сервер також відноситься до системи хмари, але на даному рисунку його було винесено з узагальненої хмарної структури для спрощеного сприйняття механізму підключення клієнтських комп'ютерів до хмарних ресурсів. Клієнтські комп'ютери через мережу зв'язку (Інтернет) з'єднуються із сервером, який обробляє запроси та керує наступними діями щодо роботи системи хмари та її взаємодією із клієнтом.

[1]Хмарні обчислення – модель забезпечення повсюдного та зручного доступу через мережу до спільного пулу обчислюваних ресурсів, що підлягають налаштуванню, які можуть бути оперативно надані та звільнені з мінімальними експлуатаційними затратами або зверненням до провайдера [1].

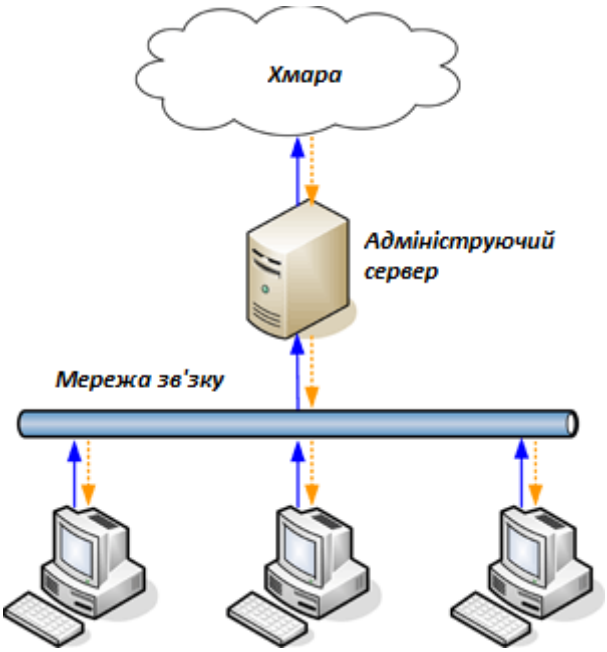

Рис.1. Спрощена модель хмари

Взаємодія між компонентами хмари

Після того, як була визначена загальна спрощена структура хмарної системи, необхідно визначити, яким чином здійснюється обмін інформацією між компонентами системи для того, щоб застосувати оптимальний механізм захищеного обміну інформацією та обґрунтувати вимоги до нього.

Визначимо головні структурні елементи хмари та взаємодію між її компонентами (рис. 2):

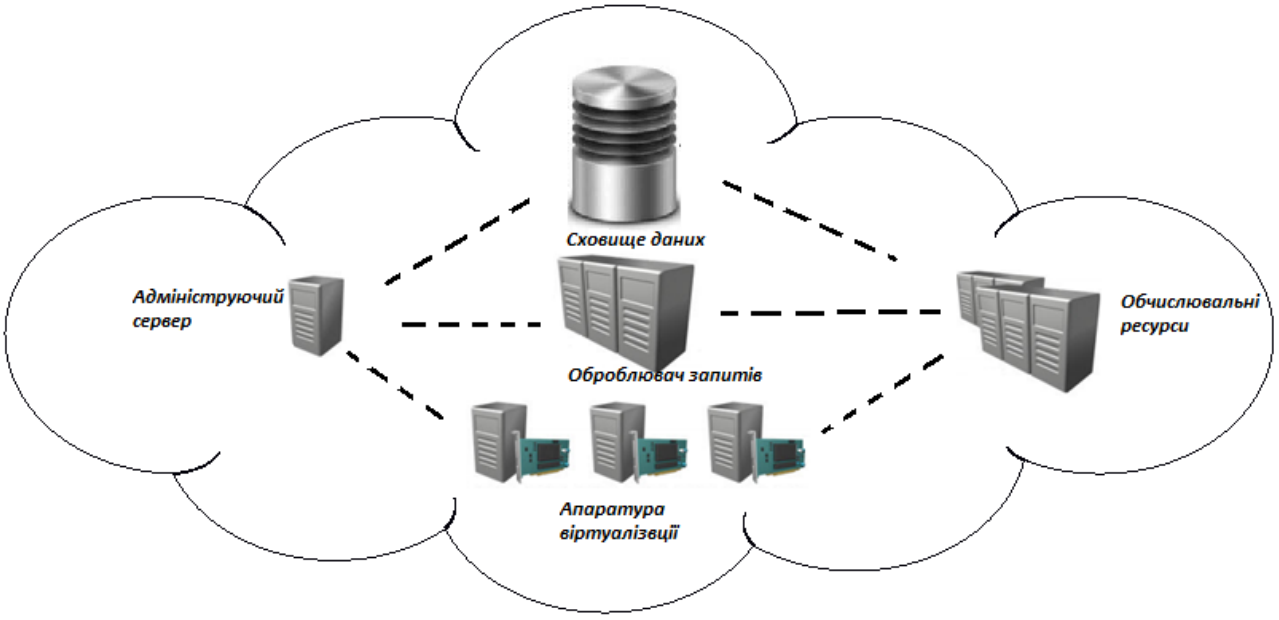

Рис. 2. Узагальнена структурна схема хмари

Таким чином, головними елементами хмари можна назвати: сховище даних, адмініструючий сервер, апаратуру віртуалізації, оброблювач запитів та обчислювальні ресурси. Всі ці компоненти можуть бути реалізовані по-різному та складатися з декількох компонентів. У процесі взаємодії інформації між компонентами системи можуть використовуватися різні дисципліни обслуговування та механізми обміну даними. Головним у процесі виступає адмініструючий сервер, який обробляє всі поступаючі до системи запити і керує їх виконанням. Після того, як запит поступає на обслуговування, наступний його маршрут визначає оброблювач запитів, який керує в якій послідовності та який сама компонент буде задіяний у процесі обробки запита. Ця концепція дозволяє більш детально визначити вимоги до протоколу захищеного обміну даними та визначити, як саме компоненти повинні виконувати ті чи інші дії [1].

Загрози порушення конфідіційності, цілісності доступності інформації

Якщо розглядати загрози порушення конфіденційності, цілісності та доступності на кожному можливому вразливому рівні системи хмари, то можна чітко прослідити та визначити вірогідності щодо атаки того чи іншого рівня та на цієї підставі виявити найбільш вразливі місця системи. Посилаючись на модель загроз системи хмарних обчислень [1] можна виділити наступні можливі загрози:

1. Відмова апаратного обладнання (дії зловмисника чи можливі перебої електропостачання);
2. Застосування шпигунського обладнання, що копіює чи модифікує оброблювані дані;
3. Аналіз побічних електромагнітних випромінювань;
4. Електротехнічні канали витоку інформації;
5. DoSатаки (перевищення кількості можливих запитів, що призводить до відказу в обслуговуванні, таким чином доступ до ресурсів хмари стає неможливим);
6. Maninthemiddle (людина всередині, тобто прослуховування та аналіз трафіка мережі без відома користувачів та системи з використанням спеціально розробленого ПЗ чи АЗ). Взагалі цей тип загрози передбачає наступні різновиди мережевих загроз:
   - видача себе за іншого користувача засобом аналізу вхідних на вихідних пакетів чи фізичне підключення до мережі;
   - прослуховування трафіку як він є;
   - перехоплення та навмисне переривання каналу передачі інформації.
7. Загрози пошкодження безпосередньо каналів зв'язку та їх компонентів (з технічної точки зори – кабелів, комутаторів та таке інше).

Метою даної роботи є визначення вимог та інших характеристик певних криптографічних методів захисту інформації; таким чином, об'єктом дослідження є саме криптографічні методи захисту інформації, тому у дослідженнях не будуть розглядатися технічні канали захисту інформації та загрози, пов'язані з ними, а саме загрози 1, 3, 4 та 7.

На основі цього задача забезпечення конфіденційності, цілісності та доступності інформації буде вирішуватися криптографічними засобами захисту інформації, тобто протоколи захищеної передачі інформації повинні вирішувати питання, що постають при захисті системи від атак 2, 5, 6 (із наведеного списку) [1].

Обгрунтування адекватності та актуальності використання механізмів захищеного обміну

Якщо головним для користувача є забезпечення конфіденційності при обчисленнях в хмарах, то найкращим засобом захисту можна назвати криптографічний захист інформації. Аналізуючи наведений вище матеріал можна обґрунтувати актуальність використання механізмів забезпечення захищеного обміну даними наступним чином. При використанні систем хмарних обчислень у споживача відсутня можливість застосування додаткових засобів обмеження доступу до інформації, таких як контроль фізичного доступу та інших організацій-

них і технічних заходів. Таким чином, складається ситуація, коли єдиним надійним контрольованим засобом захисту інформації може стати криптографічний засіб. Адекватним є використання модулів шифрування, цифрових підписів та протоколів захищеного обміну даними. Всі ці методи можна об'єднати спеціальними системами або програмними компонентами, які в цілому можна назвати механізмом забезпечення захищеного обміну інформацією. До переваг таких механізмів можна віднести наступне:

- криптографічна безпека встановлюваного з'єднання;
- відкритість програмного коду, що дає можливість програмістам вдосконалювати протокол до певного рівня та розробляти додатки до нього;
- розширюваність, що згодом надасть можливість використовувати нові криптографічні алгоритми та геш-функції;
- відносна ефективність, яка обґрунтовується завдяки спеціальній технології зменшення активності робочої машини, що використовується майже у всіх протоколах поданого типу [2].

Таким чином, механізми захищеного обміну інформацією є дуже зручним та адекватним рішенням проблеми забезпечення надійного та конфіденційного обміну даними при обчисленнях в хмарі. Крім наведених переваг, такі механізми відповідають головним вимогам до технології безпечного обміну даними. Основними та визначними вимогами з яких є:

1. Забезпечення КЦД[2] на всіх етапах взаємодії з інформацією у хмарі.
2. Ефективність роботи механізму, тобто досягнення забезпечення КЦД витратою адекватної кількості ресурсів.
3. Можливість поширеного впровадження з урахуванням різного типу апаратного забезпечення.
4. Використання сертифікатів для ідентифікації та автентифікації.

В результаті можна зробити висновок, що використання механізму захищеного обміну даними є актуальним та адекватним для вирішення поставленого питання про забезпечення КЦД при обробці інформації хмарою [3].

Узагальнений опис пропонованого протоколу обміну даними

На основі попередніх досліджень та аналізу вимог до механізмів забезпечення надійного обміну інформацією можна зробити вибір оптимального протоколу, що буде задовольняти всім заявленим умовам та володіє всіма необхідними властивостями. Одним з таких сучасних протоколів є ECIES(Elliptic Curve Integrated Encryption Scheme) [4].

Криптосистема (механізм) ECIES реалізує направлене шифрування і розроблена при виконанні проекту NESSIECerticomCorp. При реалізації механізму необхідно [5] :

- отримати справжні загальні параметри для еліптичної кривої;
- кожен абонент генерує асиметричну пару ключів;
- реалізується зашифрування повідомлення та виробляється код автентифікації для криптограми;
- здійснюється контроль цілісності прийнятої криптограми.

Узагальнено алгоритм роботи криптосистеми представлено на (рис. 3). Головною перевагою даної системи розробники вважають її ефективність роботи. Вона досягається завдяки механізмам, які забезпечують розумне розділення етапів роботи алгоритму між собою, що ґрунтується на стані певних параметрів системи у конкретний час. Інші переваги, недоліки та детальний алгоритм роботи механізму розглянуто у роботах [4, 5].

[2]КЦД – конфіденційність, цілісність, доступність

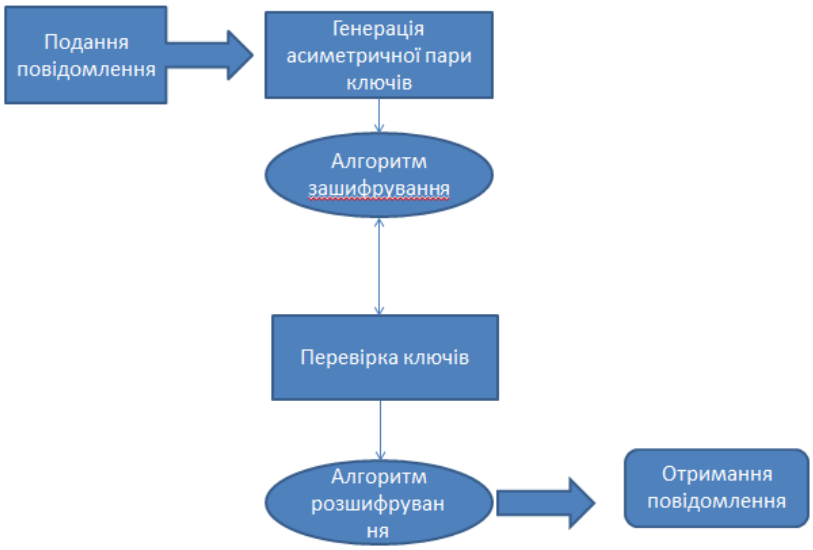

Рис. 3. Спрощена блок-схема роботи ECIES

Висновки

Робота з хмарними технологіями на сьогоднішній день вимушує більш ретельно ставитися до питань забезпечення безпеки обробки даних. Найбільш адекватними та надійними на даний момент вважаються криптографічні методи захисту інформації, які забезпечують КЦД на відповідному рівні.

Механізми захищеного обміну даними також належать до криптографічних методів захисту інформації, бо складаються з окремих модулів шифрування, сертифікації, автентифікації та направленого шифрування. При виборі певного протоколу такого типу головною є об'єктивна оцінка характеристик кожного з модулів.

Це позначає, що стійкість механізму визначається стійкістю обраних алгоритму шифрування, геш-функції, протоколу обміну ключами та інше. Одним з сучасних алгоритмів такого типу, що відповідають потрібним умовам, є криптосистема ECIES, що використовує перетворення в групі точок еліптичної кривої, провідні алгоритми шифрування та асиметричний протокол обміну ключами.

Більш детальний опис, обґрунтування адекватності вибору механізму та його оцінки планується зробити у подальших роботах.

Список літератури: 1. *Хмарні* обчислення та аналіз інформаційної безпеки у хмарі /І.Ф.Аулов, І.Д.Горбенко // Прикладна радіоелектроніка. – 2013. – Т. 12, №2. – С.194-201. 2.*Електронний* ресурс: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdfhttps://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf 3.T.Mather, S.Kumaraswamy,S.Latif,Cloud Security and Privacy:An Enterprise Perspectiveon Risks and Compiliance, O`ReillyMedia,2009.-334c. 4. *Електронний* ресурс: http://www.cryptopp.com/wiki/Elliptic_Curve_Integrated_Encryption_Scheme 5. *Конспект* лекцій з прикладної криптології.-13 Лк/ І.Д.Горбенко

Харківський національний університет
ім. В.Н. Каразіна

Надійшла до редколегії 12.02.2014