УДК 004.75

к.т.н., доц. **Бойчук В.О.** (ХмНУ)
д.т.н., проф. **Лєнков С.В.** (ВІКНУ)
Нікіткін О.М. (ХмНУ)

КРИПТОГРАФІЧНИЙ МЕТОД ОПТИМІЗАЦІЇ РОБОТИ ВІДДАЛЕНИХ СЕРВІСІВ НА БАЗІ РОЗПОДІЛЕНИХ СИСТЕМ

Сьогодні хмарними обчисленнями не здивуєш нікого: вони скрізь і всюди. А в умовах світової фінансової кризи багато великих компаній, спочатку не звертаючі уваги на хмарні сервіси та послуги, різко перенаправили свої грошові потоки саме туди, усвідомивши давні помилки і прорахунки. У цій статті розглянуто інформацію про переваги та проблеми в сервісах на основі розділених систем, так званих - cloud-сервісах. Також розглянуто криптографічний спосіб вирішення проблем безпеки даних користувачів хмарних сервісів.

Ключові слова: cloud-сервіс, хмарні обчислення, Software as a Service (SaaS), криптографічні методи.

Вступ. Сервіси на базі розподілених систем охоплюють великий спектр різних обчислювальних ресурсів і послуг, що використовуються користувачами через Інтернет. Такі рішення дозволяють будувати інформаційні системи для управління без придбання дорогого устаткування. Це дає можливість споживачам вирішити проблеми несанкціонованого використання програмного забезпечення, а також знизити великий відсоток витрат на побудову центрів обробки даних. Хмарні технології мають можливість миттєво реагувати на збільшення попиту, що дозволяє вирішити питання, пов'язані з тривалим часом побудови та введення в експлуатацію великих об'єктів IT-інфраструктури [4].

Постановка проблеми. У щорічному дослідженні Gartner, проведеному серед IT-директорів і стосується інвестицій в технології, хмарні обчислення різко перемістилися з шістнадцятої позиції на другу. І зараз основним завданням є забезпечення безпеки цих сервісів. Справді, переважна більшість клієнтів, дізнавшись про хмару, кажуть, що вони скоріше створять віртуальний центр обробки даних на своїй території, так звані приватні хмарні сервіси, оскільки погано знайомі з питаннями безпеки.

У зв'язку з цим забезпечення безпеки хмарних обчислень буде основним напрямком діяльності вендорів в найближчому майбутньому», - вважає Джонатан Пенн (Jonathan Penn), аналітик Forrester Research. «Розробники, що займаються безпекою, звикли продавати свої продукти безпосередньо підприємствам. Проте з часом вони будуть використовувати хмарних провайдерів для поставки своїх продуктів на ринок», - додає він [5].

В статті буде розглянута модель - SaaS (Software as a Service).

У моделі SaaS додаток запускається на «хмарній» інфраструктурі і є доступним через веб-браузер. Клієнт не керує мережею, серверами, операційними системами, зберіганням даних і навіть деякими можливостями додатків. З цієї причини в моделі SaaS основний обов'язок по забезпеченню безпеки практично повністю лягає на провайдерів.

Є кілька ризиків безпеки при використанні SaaS, які необхідно враховувати при прийнятті рішення про перехід на таку модель роботи.

Виклад основного матеріалу досліджень. Клаудкомп’ютинг (англ. Cloudcomputing) - це програмно-апаратне забезпечення, доступне користувачеві через мережу Інтернет, або локальну мережу, у вигляді сервісу, що дозволяє використовувати зручний інтерфейс для віддаленого доступу до виділених ресурсів (обчислювальних ресурсів, програм і даних). Користувач має доступ до власних даних, але не може керувати операційною системою і власне ПЗ, з яким він працює.

Існують такі варіанти надання сервісу клаудкомп’ютингу:

1. SaaS (Software as a Service), або програми у вигляді сервісів - варіант, при якому користувачу пропонують використовувати якесь конкретне ПЗ, наприклад, корпоративні системи, у вигляді сервісу за передплатою.

2. PaaS (Platform as a Service) - на відміну від SaaS, призначений більше для кінцевого користувача, є варіантом для розробників програм і ПЗ.

3. IaaS (Infrastructure as a Service) - дозволяє користувачам самостійно управляти ресурсами, надаючи в оренду як апаратні засоби (сервери, клієнтські системи, мережеве обладнання і так далі), так і операційні системи і необхідне прикладне програмне забезпечення [1].

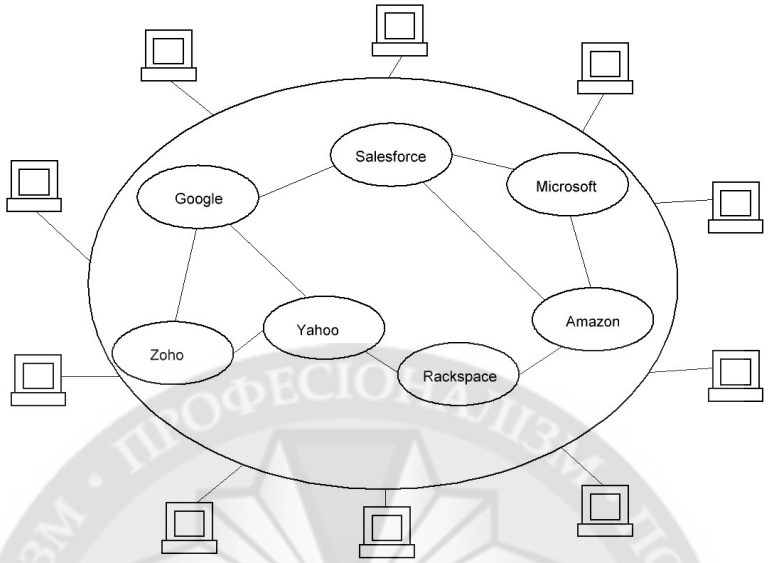

Рис. 1. Логічна схема cloud computing

Робота сервісів надається провайдерами і пов'язана з дуже великими системами. Вони мають складні процеси і вимагають висококваліфікований персонал для експлуатації систем, кожен з яких окремо не може мати повний доступ до інформаційних ресурсів в цілому. В результаті, існує безліч прямих і непрямих переваг інформаційної безпеки при використанні хмарних технологій. Тут наводяться деякі ключові переваги безпеки даних в хмарних середовищах:

1. Централізація даних: в хмарному середовищі, сервіс-провайдер піклується про питання зберігання даних, і малому бізнесу немає необхідності витрачати багато грошей на апаратну складову зберігання даних. Крім того, зберігання даних у хмарі, а отже можливість централізованого зберігання, може забезпечити обробку даних швидше і, як правило, дешевше. Це особливо корисно для малого бізнесу, який не має можливості витрачати додаткові гроші на фахівців з безпеки та адміністрування систем зберігання даних.

2. Реагування на інциденти: Постачальники IaaS послуги можуть підняти виділений «контрольний сервер», який може використовуватися на вимогу. Всякий раз, коли зафіксовано порушення безпеки, сервер може бути піднято в статус онлайн. У деяких випадках резервна копія сервісу може бути легко згенеровано і поміщена на хмару, не зачіпаючи нормальний хід бізнесу, тим самим не порушуючи безперервності бізнесу.

3. Контрольний час перевірки зображення (FIVT): Деякі реалізації хмарних технологій зберігання даних піддаються додатковим захистах із застосуванням криптографічних атрибутів таких як: визначення контрольної суми або обчислення хеш-функції. Наприклад, Amazon S3 обчислює MD5 (Message-Digest Algorithm 5) автоматично при збереженні об'єкта. Тому в теорії, зовнішні інструменти, що вимагають багато часів на генерування контрольних сум MD5, усувається.

4. Облік: У традиційній моделі обчислювальних систем, облік часто здійснюється заднім числом. Загалом, недостатність виділеного місця на диску робить його або не існуючим, або мінімальним. Однак, в хмарі, потреба зберігання в стандартних логах автоматично вирішена.

Незважаючи на всі переваги безпеки, хмарні технології не позбавлені ряду проблем інформаційної безпеки:

1. Розташування даних: Концепція реалізації хмарних технологій заснована на тому, що користувачі не знають про точне місцезнаходження центрів обробки даних, а також не мають ніякого контролю над фізичним доступом до цих даних. Найбільш відомі провайдерам хмарних сервісів мають центри обробки даних по всьому світу. Деякі постачальники послуг також можуть скористатися своїми глобальними центрами обробки даних. Проте, в деяких випадках, додатки і дані можуть зберігатися в країнах, де останні мають свої судові інтереси. Наприклад, якщо для користувача дані зберігаються в країні X, то постачальники послуг будуть піддаватися вимогам безпеки та правовим зобов'язанням країни X, що, як правило, ускладнює діяльність користувача, який не знайомий з юридичними витратами даної країни.

2. Розслідування: Розслідування незаконної діяльності може бути неможливо в хмарному середовищі. Хмарні сервіси особливо важко розслідувати, так як дані для декількох клієнтів можуть бути розподілені і можуть також бути розміщені на багатьох центрах обробки даних. Користувачі мають мало інформації про топологію мережі, що лежить в основі середовища. Постачальник послуг також може накладати обмеження на мережеву безпеку користувачів послуг.

3. Довгострокова життєздатність: Постачальники послуг повинні забезпечити безпеку даних у випадках можливої зміни свого юридичного статусу, таких як злиття і поглинання. Клієнти повинні забезпечуватися даними в таких ситуаціях. Постачальники послуг також повинні переконатися, що дані в безпеці при негативних кондиціях, таких як тривалі відключення і просто і т.д.

4. Відповідність нормативам: Традиційні постачальники послуг піддаються перевіркам зовнішніх аудиторів та сертифікати безпеки. Якщо постачальник хмарних сервісів не дотримуються цих аудити, що в даний час не заборонено, то це призводить до очевидного зниження довіри з боку клієнтів.

5. Відновлення: Провайдери хмарних послуг повинні забезпечити безпеку даних у разі природних і техногенних катастроф. Як правило, це досягається реплікацією даних на декількох вузлах. Однак у випадку будь-якого такого небажаного події, постачальник повинен зробити повне і швидке відновлення.

6. Дані сегрегації: Дані в хмарі, при використанні глобальної хмари, розташовуються разом з даними інших клієнтів. Шифрування не може бути єдиною можливою панацеєю вирішення проблеми інформаційної безпеки. Це пов'язано з сегрегацією даними. У деяких ситуаціях, клієнти можуть не хотіти зашифровувати свої дані, через імовірність пошкодження даних при збої шифрування [2].

Для вирішення проблеми з сегрегацією даних потрібно створити такий метод, щоб при шифруванні даних були мінімальні втрати інформації, або зовсім без втрат.

Так склалося, що людині необхідно працювати з інформацією: вміти здійснювати її пошук, обробку, засвоєння, вирішувати питання, пов'язані із її зберіганням. На щастя, на сьогоднішній день є багато сервісів, які полегшують життя і допомагають долати певні труднощі. Однак вони можуть не завжди відповідати вимогам клієнтів. Наприклад, не всі пошукові системи на даний момент підтримують приватний пошук, тобто пошук, при якому пошуковий сервер нічого не знає про те, які запити надсилають йому користувачі. Хоча така річ дуже б знадобилася людям, охочим зберегти конфіденційність своїх інтересів.

Найкращим вирішенням вищеописаної проблеми була б передача даних з сервера користувачеві. Тоді власник бази точно не дізнається, що саме потрібно запитувачу. Але а що, якщо багато? Якщо їх ще потрібно шифрувати? Стискати? З'являються серйозні проблеми, пов'язані з часом і ресурсами. Але тут нам приходить на допомогу гомоморфне шифрування.

Гомоморфне шифрування - форма шифрування, що дозволяє виробляти певні математичні дії із зашифрованим текстом і отримувати зашифрований результат, який відповідає результату операцій, що виконуються з відкритим текстом. Наприклад, одна людина могла б скласти два зашифрованих числа, а потім інша людина могла б

розшифрувати результат, не використовуючи ні одне з них. Гомоморфне шифрування дозволило б об'єднати в одне ціле різні послуги, не надаючи дані для кожної послуги.

Розрізняють частково гомоморфні і повністю гомоморфні криптосистеми. У той час як частково гомоморфна система дозволяє проводити одночасно тільки одну з операцій - додавання множення, повністю гомоморфні криптосистеми підтримують одночасне виконання обох операцій, що дозволяє гомоморфно обчислювати довільні логічні контури.

Для простоти припустимо, що на якомусь сервері зберігається n-бітовий вектор x, а клієнту необхідно дізнатися і-ий біт, та так, щоб його запит був конфіденційним. Користувач відсилає серверу зашифрований бінарний вектор, кожен біт якого — зашифрований нуль (природно, з допомогою гомоморфного алгоритму), крім і-го біта. На сервері тоді виконується скалярне множення отриманого вектора x. Результат передається клієнту, який просто розшифровує надходжені дані і отримує відповідь на свій запит [3].

Висновки. Зроблені висновки про доцільність використання гомоморфного методу шифрування в віддалених сервісах на базі розподілених систем. Проведений аналіз дозволив зробити висновки про доцільність використання цього методу для захищення інформації від зловмисників.

Запропонований підхід дозволить усунути ряд недоліків при збереженні інформації в хмарних сервісах.

ЛІТЕРАТУРА:

1. Фінгер П. Бізнес платформа 21го століття, побудована на cloud computing / Фінгер Пітер. – Л. : Meghan-Kiffer Press, 2009. – 256 с.

2. Риз Дж. Облачные вычисления / Риз Джордж. – СПб.: БХВ-Петербург, 2011. — 288 с.

3. Кренделев С.Ф. Гомоморфное шифрование (защищенные облачные вычисления) / Кренделев С.Ф. – М. : Лаборатория Параллелс-НГУ, 2012 – 20 с.

4. Columbus L. Roundup Of Cloud Computing Forecasts And Market Estimates / Columbus Louis. – N.Y. : Cloud Resolutions, 2014

5. Пенн Д. Новости по Cloud Computing – Penn's Blog URL: http://www.pbuk.uk/cc.html

Без рецензії.

к.т.н., доц. Бойчук В.А., д.т.н., проф. Ленков С.В., Никиткин А.Н.

КРИПТОГРАФИЧЕСКИЙ МЕТОД ОПТИМИЗАЦИИ РАБОТЫ УДАЛЕННЫХ СЕРВИСОВ НА БАЗЕ РАСПРЕДЕЛЕННЫХ СИСТЕМ

Сегодня облачными вычислениями не удивишь никого: они везде и повсюду. А в условиях мирового финансового кризиса многие крупные компании, сначала не обращая внимания на облачные сервисы и услуги, резко перенаправили свои денежные потоки именно туда, осознав давние ошибки и просчеты. В этой статье рассмотрена информация о преимуществах и проблемах в сервисах на основе разделенных систем, так называемых - cloud-сервисах. Также рассмотрен криптографический способ решения проблем безопасности данных пользователей облачных сервисов.

Ключевые слова: cloud-сервис, облачные вычисления, Software as a Service (SaaS), криптографические методы.

Ph.D. Boychuk V.O., Prof. Lenkov S.V., Nikitkin O.M.

CRYPTOGRAPHIC METHOD OF OPTIMIZATION OF REMOTE SERVICES BASED ON DISTRIBUTED SYSTEMS

Today the cloud computing will not surprise anyone: they are everywhere. And amid the global financial crisis, many large companies, initially oblivious to the "cloud" services and services, dramatically redirected their cash flow is there, realizing the long-standing mistakes and miscalculations. In this article the information about the benefits and challenges in services on the basis of separated systems, the so-called - cloud-services. Will be considered by a cryptographic method of solving the data security of users of cloud services.

Keywords: cloud-service, cloud computing, Software as a Service (SaaS), cryptographic methods.