Кібернетика та системний аналіз

УДК 004.738.5

Т.Г. Білова, В.О. Ярута, В.В. Побіженко

Харківська державна академія культури, Харків

МЕТОДИ ПІДВИЩЕННЯ БЕЗПЕКИ ОБРОБКИ ДАНИХ В ХМАРНИХ ОБЧИСЛЕННЯХ

Розглянуто переваги та недоліки різних рівнів шифрування даних в хмарі. Проаналізовано підходи до шифрування інформації, що пропонують хмарні провайдери. Досліджено можливість використання методів гомоморфного шифрування в хмарних обчисленнях. Визначені вимоги до алгоритмів гомоморфного шифрування при обробці зашифрованої інформації в хмарі.

***Ключові слова**: хмарні технології, безпека даних, алгоритми шифрування, гомоморфне шифрування.*

Вступ

Постановка задачі та аналіз досліджень. Хмарні обчислення – нова перспективна технологія розміщення, надання та споживання додатків і комп'ютерних ресурсів, при якому вони стають доступні через Інтернет у вигляді сервісів, розташованих на різних платформах і пристроях.

Основними характеристиками хмарних обчислень є масштабованість, еластичність, мобільність, необмежений обсяг даних, що оброблюються, та можливість нарощувати ресурси [1, 2]. Але невирішеним залишається питання збереження контролю над конфіденційною інформацією, і це значно обмежує використання цієї технології для побудови інформаційних систем, які потребують особливих заходів по забезпеченню секретності.

Актуальним є аналіз існуючих підходів до забезпечення конфіденційності обробки даних в хмарі та визначення шляхів підвищення інформаційної безпеки хмарних обчислень.

Мета та завдання дослідження. *Метою* даного дослідження є оцінка можливостей використання гомоморфних методів шифрування для підвищення надійності захисту конфіденційних даних в хмарі.

У відповідності з поставленою метою слід вирішити наступні *завдання*: розглянути основні переваги та недоліки різних рівнів шифрування даних в хмарі; проаналізувати рішення по шифруванню даних, що пропонують хмарні провайдери; визначити основні вимоги до алгоритмів гомоморфного шифрування в хмарі.

Основна частина

Шифрування даних і управління ключами шифрування, що переміщуються в хмарне середовище або зберігаються в центрі обробки даних – необхідна умова для забезпечення конфіденційності даних і дотримання нормативних вимог. Але використання найбільш надійних алгоритмів шифрування значно знижує продуктивність хмарних обчислень. Розглянемо недоліки та переваги основних рівнів шифрування даних [3].

1. Шифрування окремого віртуального диску – захищає від витоку інформації на стороні провайдера (наприклад, під час резервного копіювання), а також атаки з боку інших користувачів. Однак якщо зловмисник проник в машину, до якої цей диск монтується, то таке шифрування захистити не зможе.

2. Шифрування записів на рівні бази даних – кодуються окремі поля таблиць, що містять найбільш цінні дані. Поля таблиці будуть зашифровані, але їх хеш, який використовується для пошуку – ні. Така схема не буде гальмувати вибірку з полів, оскільки дешифрування при цьому не відбувається.

3. Шифрування віртуальних машин при передачі між їх вузлами і при зберіганні в неактивному стані – на рівні гіпервізора, тобто самим виробником систем віртуалізації. Поки таких рішень немає.

4. Шифрування каналів зв'язку – наприклад, протокол SSL з апаратним прискорювачем на вході в хмару. Більш правильною архітектурою є SSL-шифрування прямо у віртуальній машині, однак це також має бути підтримано на рівні гіпервізора або його віртуального мережевого драйвера.

5. Шифрування на клієнті – найнадійніша форма шифрування, але потребує виконання обробки даних на клієнті. Це значно знижує переваги від використання хмари, тому таким чином шифрують тільки найбільш цінні дані. При цьому ключі шифрування зберігаються тільки на клієнті і передаються в хмару при авторизації. Проблемою стає організація гарантованого знищення цих ключів з часом. Вихід – використання тимчасово-

го ключа, дія якого поширюється тільки на обмежений інтервал часу.

Кожен з перерахованих методів шифрування вимагає індивідуального підходу до програмування і власних механізмів розподілу ключів. Для захисту даних в хмарних обчисленнях необхідно вибудовувати комплексну систему шифрування зі своїми специфічними протоколами.

Провайдери хмарних послуг пропонують наступні рішення для підвищення безпеки обробки даних:

1. Установлення захищеного каналу для з'єднання (наприклад, VPN – віртуальні приватні мережі). Рівень довіри до каналу залишається високим завдяки використанню засобів криптографії (шифрування, аутентифікації, інфраструктури з відкритими ключами і запобігання зміни переданих даних). Є найбільш простим і дуже дієвим рішенням, але дозволяє захистити лише канал зв'язку між користувачем та хмарою.

2. Використання поділу ролей для доступу до інформації, наприклад, адміністратора віртуальної інфраструктури та адміністратора безпеки. Це дозволяє розділити обов'язки всередині хмари. Такий поділ здійснюється провайдером, і у користувача хмарних послуг немає можливостей на нього впливати та/або контролювати.

3. Сегментування віртуальних машин – поділ віртуальних машин на сегменти для забезпечення поділу клієнтів і безпеки. Забезпечує повне розділення мережевого трафіку і поділ політиками управління доступом, навіть якщо вони працюють на загальному фізичному обладнанні і з загальною мережевою інфраструктурою. У разі створення приватної хмари це дозволяє розділити, наприклад, на сегменти віртуальні машини, що відносяться до бухгалтерії, та що відносяться до відділу розробки. Є можливість виділити ці сегменти для роботи на різних мережевих інтерфейсах.

4. Зберігання інформації в хмарі в зашифрованому вигляді – шифрування криптографічними засобами кожного файлу, який передається в хмару на зберігання. Доступ до такої інформації можуть отримати тільки ті особи, які володіють ключем для розшифрування. Даний спосіб добре зарекомендував себе для приватних осіб або малих організацій, однак при великій кількості власників ключа контролювати його використання стає проблематично.

5. Використання проміжного (проксі) сервера для шифрування даних – використовується обладнання, що знаходиться у довіреному середовищі. Сервер відповідає за шифрування всіх даних перед відправленням їх в хмару і розшифрування при запиті цих даних. Журнал обліку доступу до інформації робить процес звернення до файлів прозорим.

6. Обробка знеособлених даних в хмарі – передається лише частина даних, яка не може бути однозначно прив'язана до сутностей, що використовуються в системі. Конфіденційна інформація знаходиться лише у довіреній зоні клієнта.

Практично усі запропоновані провайдерами механізми мають уразливі місця, які можуть критично впливати на безпеку обробки конфіденційних даних. Повна довіра провайдерам хмарних послуг неможлива, тому як користувачі хмарних послуг не можуть впливати на те, що відбувається в хмарі. Виходом може стати передача даних в зашифрованому вигляді з тим, щоб операції, які здійснюються над цими даними, жодним чином не поширювали інформацію про дані. Т

оді алгоритм взаємодії с хмарою повинен включати такі кроки:

1. Дані передаються в хмару в зашифрованому вигляді.

2. Відправляється запит на виконання деяких операцій над цими даними.

3. Програма, що знаходиться в хмарі, реалізує обчислення над даними без їх дешифрування.

4. Оброблені дані повертаються організації.

5. Організація розшифровує результат.

Такий механізм захищеної обробки даних можна забезпечити лише за допомогою гомоморфного шифрування – криптографічного примітива, що представляє собою функцію шифрування, яка задовольняє додатковій вимозі гомоморфності щодо будь-яких алгебраїчних операцій над відкритим текстом [4-6].

Проаналізуємо основні поняття, пов’язані з гомоморфним шифруванням [4]. Нехай E(k,m) – функція шифрування, де k – ключ шифрування, а m – відкритий текст. Функція вважається гомоморфною щодо операції op, якщо існує ефективний алгоритм M, такий, що для будь-яких m_1 і m_2 M(E(k,m_1), E(k,m_1)) алгоритм видасть закритий текст, при дешифруванні якого буде отриманий відкритий текст m_1 op m_2.

Таку систему обчислень над зашифрованими даними можна було б легко реалізувати, якби існувала функція шифрування, гомоморфна відразу щодо двох операцій: І та АБО в разі булевих операндів, або додавання і множення у випадку числових даних. Однак питання про існування таких функцій гомоморфного шифрування, так само як і систем обчислень над зашифрованими даними, залишається відкритим [5].

Як правило, розглядається окремий випадок гомоморфного шифрування. Для функції шифрування E і операції op_1 над відкритим текстом існує операція op_2 над закритим текстом така, що при E(k,m_1) op_2 E(k,m_1) при дешифруванні виходить відкритий текст m_1 op_1 m_2.

Задачу обчислення можна розглядати в різних постановках. Наприклад, дані можуть порівнюватися за значенням, тобто якщо $m_1<m_2$, де m_1 і m_2 - відкриті тексти, то $F(k,m_1)< F(k,m_1)$. Але в загальному випадку розглядаються операції додавання і множення, тобто $E(k,m_1)$ ор $E(k,m_1)$ при дешифруванні призводять до $m_1+ m_2$ і $m_1\times m_2$.

Однією з істотних проблем відомих повністю гомоморфних криптосистем є їх низька продуктивність. В даний час існує два основні шляхи її підвищення: використання "обмеженого гомоморфізму" та "метод упаковки шифротексту" [6]. Перший має на увазі криптосистему, яка може виконувати операції двох видів (додавання і множення), але в обмеженій кількості. Суть другого в тому, що в один шифротекст записується відразу кілька відкритих текстів, і при цьому в процесі одиночної операції такого пакетного шифротекста відбувається одночасна обробка всіх його складових частин.

Але лише повністю гомоморфне шифрування здатне виключити необхідність хоча б часткової розшифровки даних для виконання обчислень над ними. Це не приведе до витіснення інших видів криптографії, оскільки будь-яке подібне шифрування принципово вразливе до атаки з підібраним текстом.

Теоретично можна вважати, що реалізація повністю гомоморфного шифрування має задовольняти наступним вимогам [4]:

1. Спектр підтримуваних математичних функцій покриває повсякденні потреби програмістів.

2. Діапазони значень чисел покривають принаймні стандартні типи даних, а обчислення, вироблені над зашифрованими даними, мають прийнятну продуктивність.

3. Точність і швидкість зберігаються протягом усіх обчислень.

4. Складність обчислення примітивних операцій над зашифрованими даними – $O(n\times\log(n))$ або $O(n)$ від потужності допустимого діапазону значень.

5. Криптостійкість алгоритму шифрування повинна бути досить велика, щоб виключити можливість атаки повним перебором.

Висновки

В перспективі найбільш ефективним рішенням для забезпечення безпеки обробки інформації в хмарі може стати гомоморфне шифрування. Але всі поширені в даний час криптографічні алгоритми не дозволяють виробляти довільні обчислення над зашифрованими даними, істотно обмежуючи можливості використання хмарних ресурсів.

Подальші дослідження у даному напрямі повинні охоплювати питання адаптації існуючих алгоритмів гоморфного шифрування до особливостей застосування їх у хмарних обчисленнях.

Список літератури

1. Білова Т.Г. Перспективи використання хмарних технологій в системах електронного документообігу / Т.Г. Білова, В.О. Ярута [Текст] // Системи обробки інформації. – Х., 2014. – Вип. 4 (120). – С. 86–89.

2. Білова Т.Г. Аналіз ризиків референтної структури хмарних обчислень / Т.Г. Білова, В.О. Ярута, І.О. Побіженко [Текст] // Наука і техніка Повітряних Сил Збройних Сил України. – 2014. – № 3 (16). – С. 144-147.

3. Шевченко П.П. Шифрование как метод обеспечения безопасности конфиденциальной информации в "облачных вычислениях" / П.П. Шевченко, Н.В. Мельников [Текст] // Материалы XXI научн.-техн. конф. "Системы безопасности – 2012". – М.: Академия ГПС МЧС России, 2012. – С. 60-62.

4. Жиров А.О. Безопасные облачные вычисления с помощью гомоморфной криптографии [Текст] / А.О. Жиров, О.В. Жирова, С.Ф. Кренделев // Безопасность информационных технологий. – М., 2013. – № 1. – С. 6-12.

5. Методы полностью гомоморфного шифрования на основе матричных полиномов / Л.К. Бабенко, Ф.Б. Буртыка, О.Б. Макаревич, А.В. Трепачева [Текст] // Вопросы кибербезопасности. – 2015. – № 1(9). – С. 14-24.

6. Банит В.В. Повышение эффективности использования шифрования RSA в облачных системах / В.В. Банит [Текст] // Молодий вчений. – 2014. – № 7 (10). – С. 10-12.

Надійшла до редколегії 1.10.2015

Рецензент: д-р техн. наук, проф. Г.Г. Асєєв, Харківська державна академія культури, Харків.

МЕТОДЫ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ ОБРАБОТКИ ДАННЫХ В ОБЛАЧНЫХ ВЫЧИСЛЕНИЯХ

Т.Г. Белова, В.А. Ярута, В.В. Побиженко

Рассмотрены преимущества и недостатки различных уровней шифрования данных в облаке. Проанализированы подходы к шифрованию информации, предлагаемые облачными провайдерами. Исследована возможность использования методов гомоморфного шифрования в облачных вычислениях. Определены требования к алгоритмам гомоморфного шифрования при обработке зашифрованной информации в облаке.

Ключевые слова: *облачные технологии, модель обслуживания, безопасность данных, шифрование данных.*

METHODS TO IMPROVE DATA SECURITY IN CLOUD COMPUTING

T.G. Belova, V.O. Yaruta, V.V. Pobizhenko

The advantages and disadvantages of the different levels of data encryption in the cloud. Approaches to the encrypted information, offering cloud providers. The possibility of using methods of homomorphic encryption in cloud computing. The requirements to the algorithms homomorphic encryption when processing the encrypted information in the cloud.

Keywords: *cloud computing, data security, data encryption, homomorphic encryption.*