УДК 004.031.43

АЛГОРИТМИ БАЛАНСУВАННЯ НАВАНТАЖЕННЯ ТА МЕТОДИ КРИПТОГРАФІЇ ДЛЯ ЗАХИСТУ ХМАРНИХ ОБЧИСЛЕНЬ В МЕРЕЖІ ДОСТАВКИ КОНТЕНТУ

Шпінталь М.Я.[1)], Дармштетер М.В.[2)], Лісогор О.О.[3)]
Тернопільський національний економічний університет
[1)] к.т.н., доцент; [2,3)] магістрант

I. Постановка проблеми

Зі збільшенням кількості користувачів проблема доставки об'ємного контенту в Інтернеті стає все більш актуальною. Виникає необхідність розташовувати сервера з даними якомога ближче до користувачів, для зменшення затримок і зниження навантаження на магістральні канали. Особливо це актуально для контенту, який потрібно одночасно роздати велику кількість користувачів.

Починаючи з століття термін "хмарні обчислення" почав активно поширюватися по світу. Основною ідеєю хмарних технологій є надання ресурсів на вимогу. Тим самим суб'єкт орендує ресурси і немає необхідності утримувати ці ресурси. Важливим питанням використання хмарних технологій є їх захист.

II. Мета роботи

Метою роботи є, на основі проведеного дослідження, запропонувати модель розподіленої мережі доставки контенту. З використанням моделі розробити алгоритми управління трафіком всередині мережі CDN для мінімізації навантаження на канал, а також вивчити можливість застосування гомоморфності криптосистем для захисту та обробки даних в хмарних обчисленнях.

III. Оптимальний розподіл копій контенту всередині CDN

Змоделюємо топологію мережі у вигляді зваженого ненаправленного графа G={V,E}. Множина вершин – множина вузлів мережі, а кожна дуга в множині E являє фізичне з'єднання між вузлами і зважено згідно деякої метрики, наприклад кількість хопів від одного вузла до іншого або інша більш складна функція яка бере до уваги пропускну здатність каналу або завантаженість вузла.

Функція *M(x)* оцінює вартість утримання копій і підтримки їх в актуальному стані та визначається як

$$M(x) = Cm\sum_{j\in Vr, c=1\ldots c} r_j^r \,, \qquad (1)$$

де Cm константа.

Мінімізація описаних функцій і визначає завдання динамічного розподілу копій і розподілу запитів. Потрібно виробити стратегію, яка створює і видаляє копії на серверах в залежності від зміни стану мережі, запитів користувачів мінімізуючи вартість і час обробки запиту.

Для вирішення цього завдання був застосований марківський процес прийняття рішень [1].

IV. Використання гомоморфного шифрування

Використання хмарних обчислень дає багато переваг, але для обробки даних в публічних «хмарах» в загальному випадку необхідно працювати з відкритими даними. Але для роботи з конфіденційними даними необхідна апаратура або хоча б організаційні заходи щодо зберігання ключів. До провайдерів хмарних обчислень такі вимоги пред’являти неможливо. Це за визначенням несе в собі ризики, так як ми не можемо вплинути жодним чином на те, як це відбувається на третій стороні. Було б набагато безпечніше передавати дані в зашифрованому вигляді з тим, щоб операції, які здійснюються над цими даними були безпечні.

Висновок

У роботі отримані наступні результати: розроблено модель мережі доставки контенту, алгоритм дозволяє рівномірно розподіляти навантаження всередині мережі доставки контенту і знизити відсоток відхилених запитів в момент пікових навантажень. Також проведено аналіз методів захисту хмарних обчислень. Виявлено що, криптосистеми RSA і Пейе можуть вузько використовуватися в додатках.

Список використаних джерел

1. Акулич И.Л. Математическое программирование в примерах и задачах. — М.: Высшая школа, 1986.
2. Sattva Q. Homomorphic encryption http://www.sattvaq.com/jai/wp-content/uploads/2013/02/Homomorphicencryption.pdf