УДК 004.056.5:004.57.2

ЗАХИСТ ІНФОРМАЦІЇ У ХМАРНИХ СИСТЕМАХ КЕРУВАННЯ БАЗАМИ ДАНИХ З ВИКОРИСТАННЯМ МЕТОДІВ АДАПТИВНОГО ШИФРУВАННЯ

Шевчук Р.П.[1)], Шміголь В.В.[2)], Коротков Д.М.[3)]
Західноукраїнський національний університет
[1)]к.т.н., доцент, [2)]магістрант, [3)]магістрант

I. Вступ

Хмарні системи керування базами даних (СКБД) надають користувачам можливість зберігання, управління та обробки даних в глобальному масштабі, зменшуючи при цьому витрати на обладнання та обслуговування [1]. Проте, разом із зростанням популярності хмарних рішень збільшується і загроза для конфіденційності даних. Інциденти з проникненням і витоками даних можуть масштабуватися на великі обсяги через розподілені середовища, що ставить під загрозу інформацію, яка міститься у базах даних [2].

У даній роботі розглядаються питання забезпечення безпеки і конфіденційності в хмарних СКБД та досліджуються методи адаптивного шифрування для захисту інформації в таких середовищах. Адаптивне шифрування дозволяє зберігати дані в зашифрованому вигляді та виконувати різноманітні операції над ними без необхідності попереднього вибору типу шифрування для кожного елемента бази даних.

У роботі представлено модель архітектури, яка базується на адаптивному шифруванні і дозволяє забезпечувати високий рівень конфіденційності даних в хмарних СКБД.

II. Мета роботи

Метою роботи є розробка та дослідження моделі архітектури для забезпечення високого рівня конфіденційності даних в хмарних СКБД з використанням методів адаптивного шифрування

III. Особливості побудови архітектури хмарної бази даних

У цій роботі пропонується архітектура хмарної бази даних, побудована на базі адаптивних методів шифрування [3]. Ця архітектура не потребує заздалегідь визначати, які операції дозволені для кожного стовпця даних, і забезпечує максимальний рівень конфіденційності для різних SQL-операцій в режимі реального часу. Незважаючи на певні обчислювальні витрати, за допомогою прототипу закодованої хмарної бази даних, у роботі показано, що адаптивне шифрування може бути успішно використане в парадигмі хмарних баз даних, оскільки більшість навантаження залишається невидимим для користувачів завдяки мережевим затримкам.

На рисунку 1 зображено запропоновану розподілену архітектуру хмарної бази даних, у якій передбачається, що незалежні та розподілені клієнти (Клієнт 1 до N) мають доступ до послуг хмарної бази даних [1-3].

Уся інформація (дані та метадані) зберігається в зашифрованому вигляді в хмарній базі даних. Запропонована архітектура керує п'ятьма типами інформації.

• Звичайні дані: інформаційний вміст, який надають користувачі клієнтів.

• Зашифровані дані: дані, які зберігаються в зашифрованому вигляді в хмарній базі даних.

• Відкриті метадані: усі дані, необхідні клієнтам для управління зашифрованими даними в хмарній базі даних.

• Зашифровані метадані: метадані, які зберігаються в зашифрованому вигляді в хмарній базі даних.

• Ключ: ключ шифрування зашифрованих метаданих. Передбачається, що він розподіляється всім законним клієнтам.

Авторизований клієнт може виконувати SQL-операції (Select, Insert, Update, Delete) у зашифрованій базі даних таотримувати відкриті метадані, розшифровуючи їх за допомогою ключа. При цьому метадані кешуються локально в реальному часі та використовуються для покращення продуктивності. Також клієнт може шифрувати запити, їх параметри та розшифровувати їх результати, використовуючи локальні відкриті метадані.

Ця архітектура гарантує конфіденційність даних в моделі безпеки, в якій мережа WAN вважається ненадійною (зловмисною), за умови, що користувачі є авторизованими.

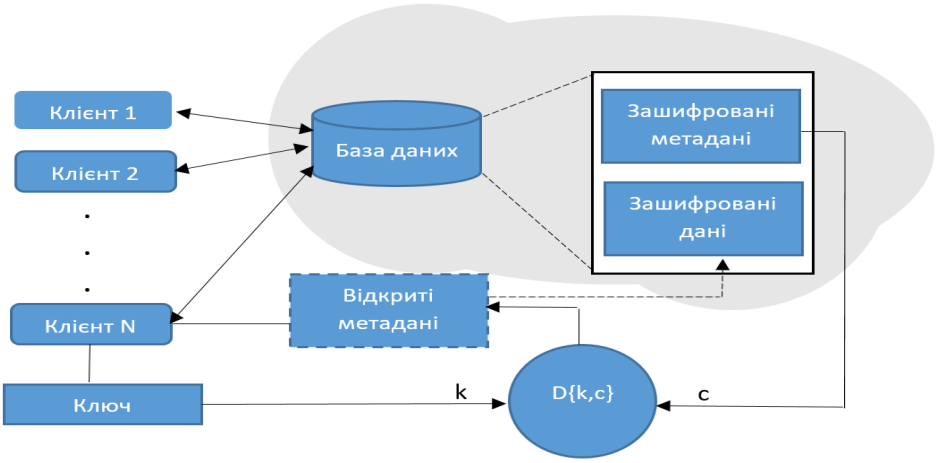

Рисунок 1 – Архітектура хмарної бази даних

На рис. 2 подано результати здійснених TPC-C транзакцій виконаних на трьох хмарних базах даних. У дослідженні брали участь 5 та 20 активних клієнтів (див. рис. 2(a) та рис. 2(b) відповідно) із різними мережевими затримками.

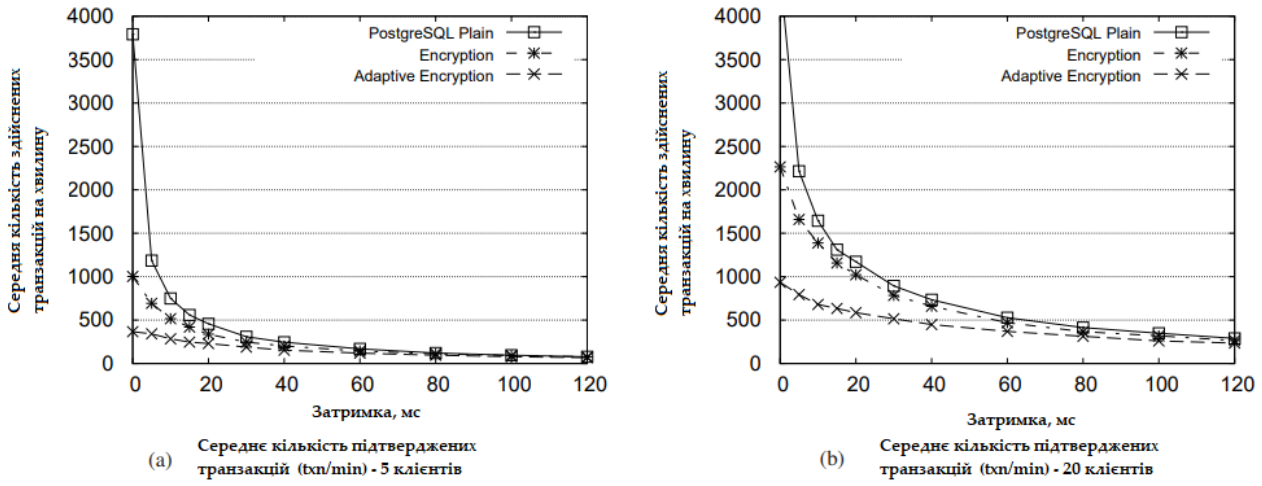

Рисунок 2 – Аналіз пропускної здатності хмарних баз даних

Результати аналізу свідчать, що в обох випадках, продуктивність виконання операцій у зашифрованій базі даних близька до продуктивності звичайної бази даних. Більше того, зі збільшенням імітованих мережевих затримок, навіть продуктивність бази даних із адаптивним шифруванням наближається до продуктивності інших двох систем і близька до продуктивності при затримках більше ніж 60 мс, які є реалістичними для типових сценаріїв хмарних баз даних.

Висновок

У даній роботі була представлена архітектура хмарної бази даних, яка ґрунтується на використанні адаптивних методів шифрування. Ця архітектура не вимагає попереднього визначення дозволених операцій для кожного стовпця даних і забезпечує максимальний рівень конфіденційності для різних SQL-операцій у режимі реального часу. Незважаючи на певні обчислювальні витрати, у роботі показано, що адаптивне шифрування може бути успішно використане в парадигмі хмарних баз даних. У результаті експериментів, щодо аналізу TPC-C транзакцій на трьох хмарних базах даних, показано, що продуктивність виконання операцій у зашифрованій базі даних практично не відрізняється від аналогічної продуктивності звичайної бази даних.

Результати дослідження підтверджують перспективи використання адаптивного шифрування в системах управління базами даних у хмарних середовищах і розкривають його можливості у забезпеченні високого рівня конфіденційності даних.

Список використаних джерел

1. Divyakant Agrawal, Amr El Abbadi, FatihEmekci and Ahmed Metwally, "(2009)Database Management as a Service: Challenges and Opportunities", *Data Engineering ICDE'09. IEEE 25th International Conference on. IEEE*, pp. 1709-1716, 2009.
2. A.Sangroya, S. Kumar, J.Dhok and V. Varma, "Towards analyzing data security risks in cloud computing environments", *Communications in Computer and Information Science*, 2010.
3. Almorsy Mohamed, John Grundy and Ingo Müller, "An analysis of the cloud computing security problem", *arXiv preprint arXiv:1609.01107*, 2016.