УДК 004.9

БЕЗПЕКА ДАНИХ ПРИ ВИКОРИСТАННІ ХМАРНИХ ОБЧИСЛЕНЬ ДЛЯ РОЗРОБКИ ПРОГРАМНИХ СИСТЕМ

***Каук В.І.**, доцент, кафедра ПІ, ХНУРЕ*
***Трибух А.О.**, студент, кафедра ПІ, ХНУРЕ*

***Анотація.** В роботі розглянуті підходи забезпечення безпеки даних в хмарі. Досліджено алгоритми роботи с зашифрованими даними. Проведено аналіз методів гомоморфного шифрування. Визначені особливості алгоритмів FHE, SHE, PHE та дана оцінка їх застосуванню на практиці.*

***Ключові слова:** ПАТЕРНИ, ХМАРНІ ТЕХНОЛОГІЇ, АЛГОРИТМ, ШИФРУВАННЯ, FULLY HOMOMORPHIC ENCRYPTION, SOMEWHAT HOMOMORPHIC ENCRYPTION, PARTIALLY HOMOMORPHIC ENCRYPTION.*

Проаналізовані та розроблені патерни та підходи для забезпечення безпеки та конфіденційності приватних даних при розробці програмних систем в хмарному середовищі. Досліджено алгоритми обчислення над зашифрованими даними в хмарі.

Розглядаючи та аналізуючи підходи для забезпечення безпеки даних в хмарі, прийшов до висновку, що їх можна розділити на декілька логічних груп. Кожна група відповідає за безпеку даних на своєму рівні. Нижче будуть перелічені ці групи:

- регуляція та відповідність законодавчим нормам;
- ідентифікація, аутентифікація та авторизація користувачів;
- приватність та конфіденційність даних;
- безпечна архітектура програмних систем.

Для більш глибокого аналізу було обрано дослідження алгоритмів, які забезпечують можливість виконання обчислень над зашифрованими даними. Необхідність виконувати такі обчислення є досить розповсюдженою та зумовлена тим, що часто виникає потреба забезпечити неможливість розкриття даних в процесі обробки, якщо вони є надзвичайно конфіденційними, як наприклад дані медичні дані пацієнтів, банківська інформація тощо.

Обчислення над зашифрованими даними, або гомоморфне шифрування, це підхід до обробки даних, коли операції виконуються без розшифрування самої інформації. Тобто, дані залишаються зашифрованими протягом всього обчислювального процесу, що дозволяє зберігати конфіденційність даних під час обробки.

В ході дослідження була проаналізована ефективність деяких методів гомоморфного шифрування. Нижче перелічені деякі з них:

- Fully Homomorphic Encryption (FHE): Цей тип шифрування дозволяє виконувати будь-які арифметичні операції (додавання, множення тощо) над зашифрованими даними;

– Somewhat Homomorphic Encryption (SHE): Цей тип шифрування дозволяє обмежений набір арифметичних операцій над зашифрованими даними, зазвичай обмежене кількістю операцій або їх складністю;

– Partially Homomorphic Encryption (PHE): Цей тип шифрування дозволяє виконувати або додавання, або множення, але не обидві операції разом.

Нижче будуть приведені висновки з порівняння даних алгоритмів.

Алгоритм FHE дозволяє нам виконувати будь-які операції над зашифрованими даними, проте він дуже затратним з точки зору обчислень і пам’яті. І перевищує усі інші розглянуті алгоритми за цими показниками більш ніж в два рази. Алгоритми SHE і PHE показали приблизно схожі результати з точки зору продуктивності, де PHE ефективніший за пам’яттю. Проте слід розуміти, що вони мають трохи різні юз-кейси використання та різні обмеження. PHE – це менш потужний за FHE або SHE, але може бути ефективним у певних випадках за рахунок простоти.

Таким чином, було зроблено аналіз існуючих алгоритмів гомоморфного шифрування та підготовлений ґрунт для подальших досліджень, щодо використання даних алгоритмів на практиці.

Література.

1. Cloud Security Patterns. Cloud Security Patterns. http://www.sirris.be.s3-website-eu-west-1.amazonaws.com/index.html.

2. O'Neill, M. (2017). Practical Homomorphic Encryption Over the Integers for Secure Computation in the Cloud. Оксфорд: IMACC.

3. AWS Lambda. https://aws.amazon.com/lambda/.