УДК 621.374.411

М. Ю. Борка
С. В. Барабан

СТРУКТУРА ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ ПЕРЕВІРКИ ЦІЛІСНОСТІ ДАНИХ У ХМАРНОМУ СЕРЕДОВИЩІ

Вінницький національний технічний університет

Анотація

В роботі доведено актуальність перевірки цілісності даних в хмарному середовищі. Описано основні методи гешування та цифрового підпису файлів, розроблено структуру інформаційної технології перевірки цілісності даних в хмарному середовищі. Доведено, що завдяки хмарним технологіям дані для перевірки містяться не на дисках або у файлах на комп'ютері, а на сервері, що не дає можливість зловмисникам переглядати дані локально.

Ключові слова: інформаційна технологія, захист файлів, цифровий підпис, гешування, SHA-3-256, AWS

Вступ

Останнім часом хмарні технології отримали широке розповсюдження та знайшли застосування у різних сферах, таких як синхронізація даних, розподілені обчислення, збереження та передача файлів, інше. Використання хмарних обчислень передбачає, що програмне забезпечення надається користувачеві у вигляді Інтернет-сервісу.

Однак використання хмарних технологій має свої недоліки. Один з головних недоліків полягає у тому, що приватна інформація користувача, зберігається на серверах хмарного провайдера, тим самим стає доступною для третьої сторони. Це може породжувати питання щодо конфіденційності та безпеки даних, особливо в разі, коли користувач не має повного контролю над інфраструктурою. Крім того, дані можуть бути вразливими під час їх передачі по каналах зв'язку, що також варто враховувати при роботі з хмарними сервісами.

Результати дослідження

Із підвищенням інтенсвності використання хмарних обчислень постає необхідність у збільшенні рівня безпеки та захисту інформації в хмарних середовищах. Запити на надійність та конфіденційність стають дедалі більшими, оскільки обсяги генерованих і зберіганих даних у хмарних сховищах зростають щороку, апроксимуючи збільшення на приблизно 60%. Це призводить до актуалізації вимог до захисту цих даних та забезпечення їх постійного доступу. Зростання обсягів інформації робить її економічним активом високої цінності [1].

За результатами здійсненого аналізу можна зробити висновок, що одним з недоліків хмарних технологій є недостатня захищеність і недостатнє забезпечення конфіденційності інформації в хмарі. Основними аспектами таких проблем є такі:

- необхідність конфіденційності зберігання даних користувача, оскільки дані не можуть бути переглянуті або змінені іншими людьми;
- необхідність збереження конфіденційність інформації під час перегляду або виконання інших операцій;
- неможливість показу та модифікації даних іншими людьми під час їх виконання (завантаження в системну пам'ять);
- необхідність конфіденційності під час передачі даних.

Для доступу користувачів до своїх даних необхідна процедура однозначної ідентифікації. Користувачі можуть отримати доступ до своєї інформації самі та/або дозволити авторизацію інших користувачів для доступу до своїх даних [2].

Отже, однією з найважливіших проблем при використанні хмарних технологій є забезпечення цілісності та істинності даних в середовищі, де інформація часто пересувається між різними платформами та системами. Це стає особливо актуальним у зв'язку з розповсюдженням розподілених обчислень та зберігання даних в хмарних середовищах.

Для вирішення цієї проблеми широко використовуються криптографічні алгоритми, зокрема алгоритми гешування. Головна мета використання таких алгоритмів полягає в тому, щоб забезпечити стійкість до змін та невідомість при передачі даних. Процес гешування конвертує вхідні дані будь-якої довжини в фіксований хеш-код фіксованої довжини, що служить унікальним ідентифікатором для цих даних.

Використання алгоритмів гешування не лише дозволяє впевнено визначити цілісність даних, але і забезпечує захист від навмисних змін чи корупції інформації. Додатково, вони застосовуються для валідації цифрових підписів та підтвердження автентичності даних під час їхнього переміщення в хмарних середовищах.

Застосування алгоритмів гешування стає ключовим елементом стратегій кібербезпеки в хмарних обчисленнях, забезпечуючи надійний механізм для збереження цілісності даних та підвищення загальної безпеки в цьому електронному середовищі [3].

Окрім цього, важливим є унеможливлювання проведення несанкціонованого дослідження вмісту даних користувача, що може бути досягнене шляхом шифрування, оскільки шифрування – це один з найбільш стійких способів захисту інформації [4].

З огляду на це, структура інформаційної технології перевірки цілісності даних в хмарному середовищі, має вигляд, як показано на рис. 1

Рисунок 1 – Структура інформаційної технології перевірки цілісності даних в хмарному середовищі

Висновки

Отже, для реалізації інформаційної технології перевірки цілісності даних у хмарному середовищі обрано алгоритм гешування SHA-3, оскільки даний алгоритм гешування є надійним і стійким до зламу, а популярні алгоритми SHA-2 та MD5 мають проблеми з надійністю, хоча і працюють швидше за алгоритм SHA-3. Цілісність даних користувача забезпечується за рахунок перевірки геш-значень файлів. При додаванні файлів на сервер створюється геш-значення файлу, яке використовується для подальшої перевірки файлів на комп'ютері. Для реалізації гешування здійснено аналіз методів гешування: CRC-8, SHA-2, MD5 і побудовано їх алгоритми. Істинність даних користувача забезпечується за рахунок цифрового підпису файлів, для чого розроблено структуру захисту даних у хмарі за рахунок використання алгоритму гешування SHA-3 та цифрового підпису. Захист від несанкціонованого дослідження досягається за рахунок необхідності авторизації – неавторизовані особи не мають доступу до серверу.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Каплун В.А., Дудатьєв А.В., Семеренко В.П., Захист програмного забезпечення, частина 1 – Вінниця, ВНТУ, 2005 – 140 с.
2. Hash Algorithm Comparison: MD5, SHA-1, SHA-2 & SHA-3 [Електронний ресурс] – режим доступу: https://codesigningstore.com/hash-algorithm-comparison

3. Поліщук В. В. Програмні технології захисту інформації : конспект лекцій. Ужгород : УжНУ, 2018. 80 с.
4. Лагун А. Е. Криптографічні системи та протоколи : нав. посібник. Львів : Видавництво Львівської політехніки, 2013. 96 с.

Борка Микола Юрійович – студент групи 2КН-22м, факультет інтелектуальних інформаційних технологій та автоматизації, Вінницький національний технічний університет, м. Вінниця.

Барабан Сергій Володимирович - к.т.н, доцент кафедри комп'ютерних наук, Вінницький національний технічний університет, м. Вінниця.