Національна Академія наук України
Академія технологічних наук України
Інженерна академія України
Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки, Україна
Університет Гліндор, м. Рексхем, Великобританія
Військова дослідницька лабораторія США, м. Аделфі, США
Інститут оборони ім. С.Лазарова, м.Софія, Болгарія
Технічний університет Лодзі, Польща
Технічний університет м. Рига, Латвія
Технологічний університет м. Таллінн, Естонія
Університет Екстрамадура, м. Бадахос, Іспанія
Гомельський державний університет ім. Ф. Скорини, Білорусь
Інститут проблем математичних машин і систем (ІПММС) НАН України
Інститут прикладної математики імені М.В. Келдиша РАН, Росія
Національний технічний університет України «Київський політехнічний інститут ім. І.Сікорського»
Полтавський національний технічний університет імені Ю. Кондратюка
Черкаський національний університет ім. Б.Хмельницького
Чернігівський національний технологічний університет

ЧОТИРНАДЦЯТА МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

МАТЕМАТИЧНЕ ТА ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ СИСТЕМ МОДС 2019

Тези доповідей

Чернігів 2019

УДК 378.04

ПРОБЛЕМИ БЕЗПЕКИ ДАНИХ У ХМАРНИХ ТЕХНОЛОГІЯХ

О.О. БОРОДІНА, А.М. ГАФІЯК, А.Є. ВИПОВСЬКА, М.С. МОДІНА

Полтавський національний технічний університет імені Юрія Кондратюка

Хмарне обчислення – це технологія галузі обчислювальної техніки, що сьогодні стрімко розвивається. Дана технологія має як багато переваг, так і декілька недоліків, пов'язаних з проблемами безпеки. Для будь-якого користувача хмарного сервісу дані є надзвичайно важливими, а їх витік може зруйнувати довіру людей та потягти за собою інші серйозні наслідки. Тому провайдери хмарних сервісів приділяють більше уваги безпеці даних.

Кожен використовує хмарне обчислення у повсякденному житті в тій чи іншій формі, навіть не підозрюючи, як-от Microsoft Office 365, Gmail, Dropbox і т. д. У хмарних обчисленнях дані зберігаються за межами місця споживача (у провайдера), тому слід застосовувати додаткові заходи безпеки, окрім традиційних перевірок, щоб забезпечити безпеку даних, а також не допустити атак хакерів та інші порушення через вразливість системи.

Життєвий цикл даних складається з шести етапів: створення, зберігання, використання, поширення, архівування та знищення [1]. Після створення дані можуть вільно пересуватися між будь-якими етапами. Дані повинні бути захищені на всіх стадіях свого життєвого циклу від їх створення до їх знищення.

Конфіденційність, цілісність та доступність є трьома важливими властивостями даних, і це популярно називають тріадою CIA [2]. Конфіденційність стосується конфіденційності даних, де вони належать споживачу, та не повідомляються стороннім особам у будь-якому випадку. Цілісність даних – це впевненість у тому, що дані, які зберігаються у хмарі, не переглядаються неавторизованими сторонами. Це також враховується, коли дані переміщуються. Цілісність передбачає підтримку точності, узгодженості та надійності даних протягом всього їхнього життєвого циклу. Доступність даних означає запоруку, що коли споживач потребує даних, дані повинні бути доступними йому без будь-якої затримки або відхилень. Ці три основні аспекти захисту даних перевірені неодноразово в моделі розгортання публічних хмар.

Важливими є правила авторизації, яка є запорукою того, що людина має доступ до своїх даних. Авторизація – це процес визначення того, чи

має людина право виконувати з даними такі дії, як читання чи редагування.

Враховуючи вищесказані особливості безпеки даних, на нашу думку, наступні кроки можуть бути використані для підтримки належної CIA у хмарних обчисленнях:

- ✓ класифікація даних після їх створення, визначення правил та методів доступу для різних типів даних;
- ✓ зберігання даних з належним фізичним та логічним захистом безпеки, включаючи резервну копію та план відновлення;
- ✓ визначення типів даних та яким чином їх можна поширити, визначення правил обміну даними. У хмарних обчисленнях багато таких правил спільно називаються Угодами про рівень обслуговування (SLA);
- ✓ створення плану виправних дій у разі пошкодження даних через мережеві або комунікаційні пристрої, дефектів безпеки під час переміщення даних;
- ✓ впровадження належних методів ідентифікації та керування доступом для користувачів до даних. Використовування дублювання даних, резервування, резервних копій та змінюваних систем для вирішення проблем доступу.

Слід зазначити, що методи шифрування, як правило, забезпечують конфіденційність від атак провайдера хмар, але не можуть захистити дані від помилок конфігурації та програмних помилок [3].

Коли з'являються нові розробки у галузі IT, завжди виникають й нові проблеми в області хмарних обчислень, що потребують вирішення. Також ряд інших проблем може виникати через їх розташування та одночасну велику кількість користувачів. У хмарних обчисленнях всі дані, особливо конфіденційні, повинні регулярно підтримуватися та перевірятися на належне відновлення даних у випадку системних помилок.

Література

1. A. Reed, C. Rezek, C and P. Simmonds. Security Guidance for Critical Area of Focus in Cloud Computing V3.0, Cloud Security Alliance (CSA), 2011, c.1-177

2.Z. Xiao and Y. Xiao. Security and Privacy in Cloud Computing, IEEE Communications Surveys & Tutorial, Vol. 15, 2012, c.843-859

3. S. Aldossary and W. Allen. Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions. International Journal of Advanced Computer Science and Applications, Vol. 7, 2016, No. 4