УДК 629,113(0711): 004.01: 004.04
Я.П. Цяпич, О.К.Каганюк , К.Я. Бортник
Луцький національний технічний університет

ПІДВИЩЕННЯ БЕЗПЕКИ І ЯКОСТІ ОБМІНУ ДАНИХ В ХМАРНИХ СЕРЕВЕРАХ

Цяпич Я.П., Каганюк О.К., Бортник К.Я. Підвищення безпеки і якості обміну даних в хмарних сереверах. В даній наукової статті досліджені механізм хмарних розрахунків, а також розглянути проблемні питання по захисту даних в хмарному серверу Була розглянута одна із моделей, яка базується на загальноприйнятих технологіях по використанню хмарних серверів, яка дозволяє збільшити якість передачі даних і забезпечити захист інформації.
Ключові слова: підвищення безпеки та якості обміну даних, хмарні технології, математична модель підвищення безпеки обміну даних, вимоги безпеки даних в хмарних обчислень, HDFS.
Форм. 0. Рис. 0. Літ. 5.

Цяпыч Я.П., Каганюк А.К., Бортник Е.Я. Повышение безопасности и качества обмена данных в облачных серверах.. В данной научной статье исследован механизм облачных вычислений, а так же рассмотрены проблемные вопросы по защите данных в облачной сервере. Была рассмотрена одна из моделей, которая базируется на общепринятых технологиях по использованию облачных серверов позволяющих увеличить качество передачи данных и обеспечить защиту информации.
Ключевые слова: повышение безопасности и качества обмена данных**,** облачние технологи, математическая модель повышения безопасности обмена данных, требования безопасности данных в облачных вычислений, HDFS.
Форм. 0. Рис. 0. Лит. 5.

Tsyapych Ya.P., Kaganiuk A.K.,Bortnik E.Y Improving the safety and quality of data exchange in the cloud sereverah. This research work investigates the mechanism of cloud computing and data protection issues in the cloud. Considered a model-based technology for the conventional cloud servers, which allows you to increase the quality of the transmission and protection in the cloud data exchange.
Keywords: improving the safety and quality of data exchange, cloud technology, mathematical model of increasing security data exchange requirements of data security in cloud computing, HDFS.
Form. 0. Fig. 0 Scr. 5.

Процеси роздільного та несинхронного розвитку двух компонентів: реального світу та кіберпространства в теперешній час придбають векторний формат, якій направлений на створення структрірованих та взаємо інтегрованих компонентів в КіберГеоСистеми. Остання еволюціонує в теперішній час створенням в кіберпросторі хмарних сервісів точного моніторингу та оптимального управління реальним світом на основі моделей, які от ображають усі земні процеси та явища. Тому створення хмарних сервісів для обчислення є **актуальною темою.**

«Хмарні» обчислення – нова глобальна парадигма обробки даних, популярність якої постійно зростає. Це стає **актуальним** для розвитку подібних технологій де приймають участь провідні світові розробники. До того ж «хмарні» сервіси розвиваються вже і в нашій країні. Ринок хмарних обчислень сьогодні величезний.

Сьогодні найпопулярнішими сервісами хмарних послуг є інтернет-додатки та віртуальні обчислювальні ресурси, які запропоновані у вигляді сервісів. Мова, яка піде в наступному розділу статті. **«Хмарні» обчислення»** – це нова модель по створенню, використанню та доставки через Інтернет IT-сервісів з використанням динамічно масштабованих і віртуалізованих ресурсів. Під масштабованістю розуміється властивість ресурсів, які використовуються по обробці інформації, або підвищення можливостей з наростаючим обсягом робіт виникаючих в процесі обробки інформації[1,3].

Після аналізу широко використовуваної технології хмарних обчислень - HDFS (HadoopDistributed File System), ми здатні сформулювати вимоги до безпеки передачі даних для хмарних обчислень. HDFS використовується в великомасштабних хмарних обчисленнях в типовій конфігурації розподіленої файлової системи. Її основна мета полягає в управлінні комерційних апаратних засобів, у зв'язку з підтримкою Google, і перевагами відкритого вихідного коду і, це дає можливість що до застосуванню обчислень в хмарних серверах..

HDFS дуже схожа на існуючу розподілену файлову систему, таку як GFS (Google File System); вони мають ідентичні цілі, продуктивність, доступність і стабільність. HDFS спочатку використовувалися в мережевий пошуковій системі Apache Nutch і стала основою проекту Apache Hadoop.

HDFS використовувала провідний резервний режим. Провідним називається «Вузол імені» (NameNode), який управляє простором імені файлів і контролює доступ до клієнта. Інший

керуючий вузол «Вузол даних» (DataNode), який контролює доступ до свого клієнта. У цій накопичувальній системі, файл поділяється на невеликі складові, «Вузол імені» відображає файлові блоки а «Вузлу даних» зверху. У той час як HDFS не володіє сумісністю POSIX, файлова система все одно старається підтримувати «створення, усунення, відкриття, закриття, читання, змінення» або інші операції з файлами.

Аналізуючи HDFS, з точки зору вимог безпеки даних до хмарних обчислень, можна розділити на наступні групи:

- Перевірка достовірності Логіна клієнта: Переважна більшість хмарних обчислень перевіряють браузер клієнта, такі як IE, і проводять ідентифікацію користувача згідно із запитом програм хмарних обчислень для первинної потреби.
- Присутність одиничної помилки з «Вузлом імені»: якщо «Вузол імені» атакують або зламують, це може привести до катастрофічних наслідків в системі. Тому ефективність «Вузла імені» в хмарних обчисленнях і його дієвість це ключ до успіху в інформаційній безпеці, тому посилення захисту «Вузла імені» дуже важливо.
- Швидке відновлення блоків даних і контроль за правом читання / запис: «Вузол даних» (DataNode) - це вузол накопичення даних, де можливі невдачі і труднощі з доступом до даних. В даний час кожен блок накопичення даних в HDFS має принаймні 3 репліки, які представляють резервну стратегію HDFS. Якщо необхідно забезпечити безпеку читання й запису даних, і HDFS не дала жодних докладних пояснень. В даному випадку необхідно забезпечити швидке відновлення з необхідністю повного контролю операції читання і запису даних, що не можливо до ігнорування даної операції.

В доповнення до трьох вищезазначених критеріїв, необхідно також враховувати і інші можливості, такі як контроль доступу, шифрування файлів, таких як попит на хмарні обчислення моделі з питань безпеки даних**.** [2]

Аналіз останніх досліджень і публікації.

Ціль даного дослідження – є моделювання алгоритму процедури підвищення якості передачі та захисту даних в хмарних обчисленнях. В даній статі передбачається можливість розроблення та визначення концепції будови нової конфігурації в обчислюванні в хмарних серверах. Нова конфігурація складається з розмаїття нових технологій, таких як Hadoop, Hbase, що підвищує продуктивність системи хмарних обчислень, але в той же час може призвести до ризику. У середовищі хмарних обчислень користувачі створюють багато динамічних віртуальних організацій, які в першу чергу ґрунтуються на довірі між організаціями більше, ніж на рівні індивідуалів. Тому з тими користувачами, які ґрунтуються на вираженні обмежень на базі стратегії підтверджень, працювати набагато важче. Це часто зустрічається на багатьох інтерактивних вузлах,де використовуються зв'язок між віртуальними машинами, є процес динамічний і непередбачуваний. Результатом розробляє мого проекту вважатиметься запропонований або розглянутий алгоритм(модель) оптимізації процесу передачі та захисту інформації при хмарних обчисленнях. Головним стримуючим фактором при роботі з хмарними ресурсами є питання безпеки – відсутність та контролю над серверами, які виконують обчислювальні процеси, є можливість витоку критично важливої інформації і пр. Серед інших стримуючих факторів можна відзначити сумніви в якості хмарних послуг, незначна кількість пропозицій, відсутність методик оцінки ефективності, неготовність змінювати підходи до IT-стратегій, неприйняття IT-персоналом (боязнь скорочень і т.п.), нерозуміння керівниками компаній переваг нових технологій.

Насамперед згадані побоювання справедливі у випадку банків та інших фінансових установ, що є об'єктом дуже жорсткого контролю з боку державних регуляторних органів. Національний банк України – головний регулятор вітчизняних банків – може дозволити їм використовувати хіба що приватні «хмари» (наприклад, для створення резервних ЦОД), але навряд чи коли-небудь дозволить використовувати «хмари» загального користування, оскільки в цьому випадку дані «розмиваються» по серверах, які знаходяться невідомо де (в географічному сенсі). У разі якщо банк захоче віддати свій приватний «хмара» на хостинг третій стороні, обов'язковою вимогою НБУ буде як мінімум самостійне (не аутсорсингове) адміністрування найважливіших програм конфіденційних даних.

А для вирішення багатьох завдань (таких, наприклад, як внутрішня бухгалтерія, CRM, HR та ін) фінансові організації цілком можуть використовувати «хмарні» обчислення вже сьогодні. З провайдером хмарних обчислень можна підписати відповідний договір про рівень обслуговування

(SLA), що передбачає серйозні фінансові штрафні санкції у випадку тих чи інших небажаних подій.[3]

Основні результати дослідження. у даній роботі розглядаются як перспектива впровадження певних удосконалень, на базі вже існуючих технологій, в безпеці та якості передачі даних в «хмарному» середовищі. Токож описується модель практичної реалізації забезпечення захисту даних під час «хмарного» обміну. Модель даних у хмарних обчисленнях можна описати за допомогою математичних формул наступним чином:

$$D_f = (\text{NameNode}); \quad (1)$$

$$K_f = f * D_f; \quad (2)$$

C(.): огляд вузлів;
D_f: розподілена матриця файлу f;
K_f: режим розподілу даних у вузлі даних;
f - файл, f можно описати як

f = {F (1), F (2), ... F (N)} що означає, що f - це множина n блоків файлів, де $F(i) \cap F(j) = \emptyset, i \neq j; I,j \in 1,2,3,\ldots n;$

D_f являється нульовою матрицею,- це L * L, де L - кількість вузлів даних.
Для підвищення безпеки даних хмарних обчислень, представляється Режим захисту даних для хмарних обчислень, який називається C2DSM. Його можна описати таким чином:

$$D_f' = C_A \text{ (Вузол імені)} \quad (3)$$

$$B_f = \text{M}.D_f' \quad (4)$$

$$K_f = \text{E}(f)D_f \quad (5)$$

C_A(.): аутентифікація доступу до Вузлу імені;
D_f : модель захисту конфіденційності матриці розподілу файлів;
M - рішення окремих матриць;
E(f) - зашифрований файл f блок за блоком, отримання зашифрованого файлового вектора.
У моделі використовувалася тришарова захисна структура системи, кожен шар якої виконує свої власні завдання для забезпечення захисту даних на всіх рівнях хмари.

- Перший шар відповідає за аутентифікацію користувачів, користувачів цифрових сертифікатів, виданих відповідними органами; управляє кодами доступу користувачів.
- Другий шар: відповідальний за шифрування даних користувача, а також захист конфіденційності користувачів певним способом.
- Третій шар: використання даних користувача для швидкого відновлення.

Захист всієї системи - це останній рівень даних користувача. За допомогою трирівневої структури аутентифікація користувача використовується для забезпечення цілісності даних. Аутентифікація користувача може керувати даними за допомогою таких операцій: додати, редагувати, видалити та ін. Якщо в системі аутентифікації користувача відбулося нелегальне втручання і небезпечний користувач входить в систему, шифрування файлів і захист конфіденційності можуть забезпечити цей рівень захисту. На цьому рівні дані користувача шифруються у випадку, якщо ключ доступу був введений нелегально, через функцію захисту конфіденційності, небезпечний користувач не зможе отримати повного доступу до інформації, що дуже важливо для захисту комерційних таємниць ділових користувачів в середовищі хмарних обчислень. Нарешті, швидке відновлення шару файлів за допомогою алгоритму відновлення дає даними користувача можливість швидко відновлюватися навіть при великих пошкодженнях.
У даній моделі виділяють наступні теореми.

- Теорема 1.

Якщо дані не в повному порядку тоді користувач, втрачає їх.
Перевірка:

D_f, якщо матриця розподілу файлів, то з формули (5), K_f є довжиною вектора L.
Якщо D_f, не в повному порядку, D_f можна перетворити в
D^*_f,D^*_f , що є (L-i) * (L-i) матрицею, i≥1;
K_f стає L-I вектором довжини, які приводять до скорочення у визначеніймоделі.

- Теорема 2.

Якщо ??∑??i=1??n??K_f (i) <n, то дані користувача будуть пошкоджені. K_f (i) позначає значення

точки і файлового вектора K_f.
Перевіримо:
$\sum_{i=1}^{n} K_f$ (i) означає кількість даних, які зберігаються у вузлі даних, з визначенням

f = {F (1), F (2), ... F (N)}, якщо F (i) не існують, i = 1,2 .... n, то приводить до помилки файлової пам'яті.

Якщо ??∑??i=1??n??K_f (i) <n, то буде i = 1,2 .... n, нехай K_f (i) = 0, F(i) не існує в f, файл

пошкоджено.

- Теорема 3.

Якщо існує матриця J, J≠M, але D_f = J.D_f , відбувається витік даних користувача.
Перевіримо:
M – матриця конфіденційності користувача. За допомогою матриці M ми можемо отримати D_f.
Якби існувала J, то незаконний користувач міг би отримати D_f за допомогою J. Тоді б стався витік особистих даних.[2]

Висновки

Розглянута вище модель дозволяє зробити деякі висновки та зауваження на рахунок безпеки та ефективності її рівнів. Також було важливим аспектом дослідження удосконалення алгоритмів та методів для підвищення безпеки обміну даних через «хмарні» сервери, що є дуже важливим при передачі конфіденційних та корпоративних даних. Можна відмітити такі основні напрацювання, висновки та рекомендації, які необхідно враховувати при підвищенні безпеки та якості даних в хмарних серверах:

• Підготовлена модель захисту даних, яка забезпечує новий рівень захисту та якості передачі даних між хмарними серверами.
• Проаналізована нова тришарова захисна структура системи, кожен шар якої виконує свої власні завдання для забезпечення захисту даних на всіх рівнях «хмари».
• Запропонована нова технологія хмарних обчислень, яка побудована на новій конфігурації і складається вже з існуючих засобів та технологій безпеки передачі даних.

- Також було наведено принципи та модель захисту даних, які служать підґрунтям для удосконалення та підвищення безпеки даних при обміні в хмарних серверах

Список використаних джерел

1. http://uk.wikipedia.org/wiki/Хмарні_обчислення
2. http://uk.wikipedia.org/wiki/Модель_захисту_даних_для_хмарних_обчислень
3. http://cbto.com.ua/library/hmarna-obrobka-danyh-mif-chy-realnist
4. Хаханова Г.В. (кандидатська, 05.12.02, 13.05.2009), науковий керівник – проф. Бараннік В.В. Структурно-каскадні методи стиску та відновлення даних в телекомунікаційних та цифрових системах реального часу;
5. Бондаренко М.Ф., Хаханов В.І., Енглезі І.П., Лобур М.В., Чумаченко С.В., Литвинова Є.І., Гузь О.А. Перспективні технології XXI століття: Облік моніторингу та управління дорожнім рухом - зелена хвиля // Україна, Одеса. С. 80-100, формат А5 (Розділ у колективній монографії).