КОМП'ЮТЕРНІ СИСТЕМИ І МЕРЕЖІ

Т. 1, № 1, 2019

https://doi.org/

УДК 004.65, 004.62

ДЕЦЕНТРАЛІЗОВАНИЙ ДОСТУП ДО ХМАРНОГО СХОВИЩА ДАНИХ

Л. О. Березко, В. П. Тат'янчук

Національний університет "Львівська політехніка",
кафедра електронних обчислювальних машин

Розглянуто питання підвищення безпеки зберігання та забезпечення конфіденційності управлінням доступом до даних у хмарних сховищах. Досліджено наявні способи контролю такого доступу. Запропоновано спосіб вдосконалення техніки шифрування, що ґрунтується на атрибутах політики шифротексту та його застосування в децентралізованій системі управління доступом до даних у багатокористувацьких хмарних системах їх зберігання. Основною метою є підвищення безпеки та конфіденційності управління хмарним сховищем даних, для якого наявне управління не відповідає всім необхідним вимогам.

Ключові слова: хмарні сховища даних, доступ, шифрування.

Вступ

Національний інститут стандартів та технологій визначив хмарні технології як "модель для забезпечення зручного доступу до мережі за запитами до спільних обчислювальних ресурсів (наприклад, мереж, серверів, сховищ, додатків та послуг), що швидко розробляються та керуються з мінімальними зусиллями без втручання постачальника послуг" [1]. Вони мають декілька моделей розгортання, а саме публічні, приватні та гібридні "хмари" [1–3].

Існують національні та міжнародні закони про зберігання даних. У США – це Health Insurance Portability and Accountability Act (HIPAA) [4], Payment Card Industry Data Security Standard (PCI DSS) [5], International Traffic in Arms Regulations (ITAR) [6] та Health Information Technology for Economic and Clinical Health Act (HITECH) [7]. Нещодавно у Європі прийнято доволі обтяжливий закон General Data Protection Regulation (GDPR) з його детальними правилами та жорсткими штрафами для всіх країн Європейського Союзу (ЄС), які диктують, що конфіденційна або приватна інформація повинна перебувати у фізичних межах країни чи регіону, з якої вони походять [8]. Чинні також Закон Великобританії про захист даних, Федеральний закон Швейцарії про захист даних та Канадський Personal Information Protection and Electronic Documents Act (PIPEDA) [9]. Отже, маємо багато різних законів про безпеку та конфіденційність даних, яких необхідно дотримуватися під час розроблення хмарної інфраструктури.

У разі використання хмарних сервісів у користувачів виникають питання, пов'язані із переміщенням власних конфіденційних даних та додатків із своїх приватних обчислювальних середовищ у "хмару", яку, як правило, спільно використовують через загальнодоступну мережу.

Трапляється несанкціонований доступ до інтерфейсів управління хмарними сервісами. Ці інтерфейси доступні для авторизованих користувачів і можливих неавторизованих зловмисників, тимчасом як у звичайних центрах опрацювання даних інтерфейси доступні тільки авторизованим адміністраторам безпосередньо або через приватні мережі.

Окрім того, доступ до управління "хмарами" звичайно здійснюється через веб-додаток та/або сервісні технології (рис. 1), тому інтерфейси управління "хмарами", з великою ймовірністю, спадкують вразливості цих технологій.

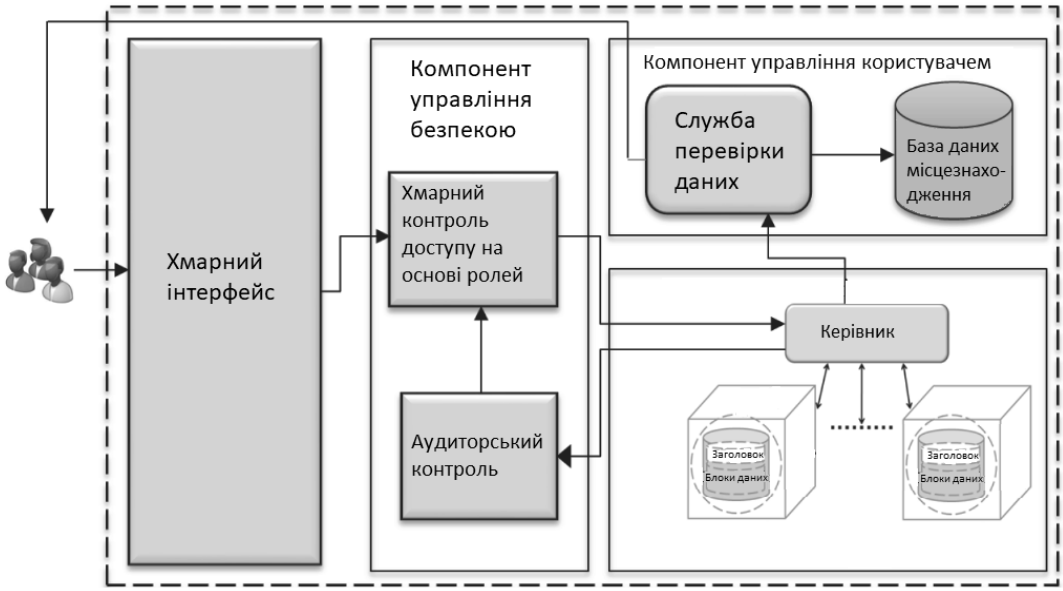

Рис. 1. Структура реалізації доступу до даних у хмарних платформах

Стан проблеми

Безпека та конфіденційність інформації в "хмарі" є принциповим питанням. Це певною мірою пов'язано з тим, що в "хмарах" немає меж, і дані, що зберігаються в "хмарі", можуть фізично розміщуватися у будь-якій точці світу або в будь-якому центрі опрацювання даних у мережі, яка географічно розподілена. Отже, використання хмарних сховищ даних зумовлює необхідність приділяти достатньо уваги проблемам безпеки та розглядати варіанти для вирішення таких питань, як конфіденційність та цілісність даних, можливості маніпуляцій та взаємодії з даними в таких сховищах. Більшість етичних питань, пов'язаних із "хмарою", стосується питань довіри та недовіри між постачальниками послуг та абонентами. Велика кількість законів стосовно конфіденційності змусила багато компаній відмовитися від зберігання даних у "хмарі", оскільки хмарні платформи не можуть гарантувати безпеку даних користувачів. Багато провайдерів можуть зберігати дані на серверах, які фізично не знаходяться в регіоні, що суперечить законам деяких країн. Це серйозна проблема для фірм у країнах, що мають чітке законодавство стосовно зберігання даних.

Служба хмарного зберігання даних дає змогу Власнику даних передавати свої дані в "хмару" і через неї забезпечувати доступ до даних для Користувача (рис. 2). Компонент Авторитет ініціалізує систему та надсилає загальнодоступні параметри (PP – public parameters) і набір усіх відкритих ключів (PK – public key) Власнику даних. Власник даних за допомогою алгоритму шифрування (Ек) генерує шифротекст (CT – ciphertext) і завантажує його на Хмарний сервер. Користувач отримує з Хмарного сервера шифротекст, отримує від Авторитету закритий ключ (SK – secret key) і за допомогою алгоритму дешифрування отримує дані, які завантажив у Хмарний сервер Власник. Алгоритм оновлення закритих ключів (UKx) потрібен тоді, коли Користувач перестав мати доступ до перегляду цих даних, оновлені закриті ключі за необхідності генерує Авторитет.

Оскільки Хмарний сервер і Власник даних, як правило, не в одному довірчому домені, у напівдовірчому Хмарному сервері не можна покладатися на застосування політики доступу. Вирішують цю проблему звичайно, примушуючи Власника даних шифрувати дані та надавати ключі шифрування авторизованим Користувачам. Але ці методи звичайно використовують складний ключ та пов'язані з накладними витратами Власника даних. Тому питання безпеки та конфіденційності у разі управління доступом до даних у хмарних сховищах даних актуальне.

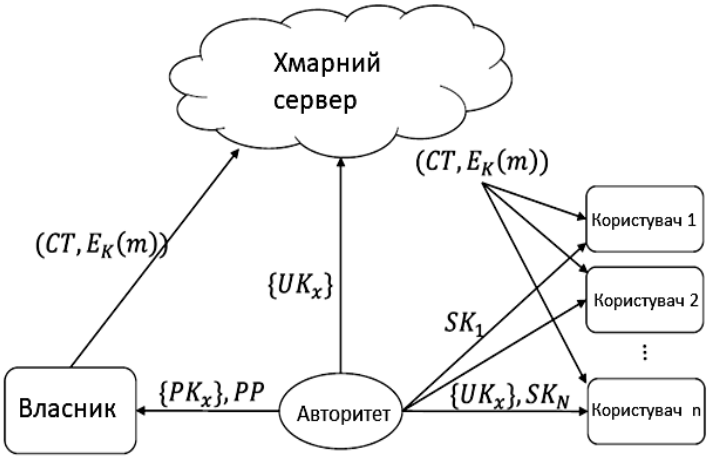

Рис. 2. Організація доступу до даних у хмарному середовищі

Постановка завдання

Оскільки метод шифрування на основі атрибутів політики шифротексту для контролю управління доступом до даних не є оптимальним для хмарних платформ, а також накладає обмеження за продуктивністю, пропонуємо децентралізовану схему управління доступом.

Розв'язання завдання

Наявна схема доступу до даних CP-ABE [10], запропонована Левко та Уотерсом, має високий рівень безпеки і надійності, але її не можна застосувати для контролю доступу у багатокористувацьких хмарних системах зберігання даних через неефективність дешифрування даних та скасування операцій. З метою розроблення ефективної схеми контролю доступу використовують вдосконалення схеми CP-ABE з ефективним дешифруванням та пропонують новий метод скасування операцій.

Нетривіальним у розробленні децентралізованої схеми CP-ABE є питання, в який спосіб зв'язати секретні ключі разом і запобігти колізійним атакам [11]. Без централізованого керування важко зв'язати разом різні компоненти секретного ключа користувача для запобігання колізійних атак. У запропонованому методі розділено повноваження для глобального центру сертифікації ключів (ЦСК) та атрибутів доступу (АД) (рис. 3). ЦСК налаштовує систему і реєструє всіх користувачів та АД у системі. Однак ЦСК не бере участі в будь-якому управлінні атрибутами та створенні секретних ключів, пов'язаних із атрибутами. ЦСК призначає глобальний ідентифікатор користувача, що відповідає індивідуальному користувачеві, та ідентифікатор глобального авторитету. Тепер він унікальний у глобальній системі, секретні ключі, видані різними АД для одного і того самого унікального ідентифікатора, можна пов'язати разом для дешифрування. Оскільки кожен АД пов'язаний за допомогою ідентифікатора, з'являється можливість протистояти колізійним атакам [11].

Для досягнення ефективного дешифрування користувач запропонував метод на основі передання позначок. Застосовується дешифрування позначки [12] та розширення її на кілька авторитетних систем, даючи змогу ЦСК генерувати глобальну пару секретного ключа та глобального відкритого ключа для кожного користувача в системі.

Під час дешифрування користувач надає свої секретні ключі, видані АД сервера, і надсилає запит сервера з метою обчислити позначку дешифрування для розшифрування шифротексту. Потім користувач може розшифрувати шифротекст, використовуючи позначку дешифрування разом із його глобальним секретним ключем.

Щоб вирішити проблему скасування атрибуту, потрібно присвоїти кожному атрибуту номер версії. У разі, коли трапляється скасування атрибуту, будуть оновлені лише ті компоненти, які пов'язані із скасованим атрибутом у секретних ключах та шифротекстах. Коли атрибут користувача можна скасувати з будь-якого АД, АД генерує новий номер версії та генерує декілька ключів оновлення користувача та ключ оновлення шифротексту. Оскільки ключі оновлення відрізняються для різних користувачів, відкликаний користувач не може оновити свій секретний ключ, використовуючи ключі оновлення інших користувачів (наявна зворотна безпека). Використовуючи ключ оновлення шифротексту, компонент, пов'язаний із відкликаним шифротекстом, може оновитися до поточної версії.

Для підвищення ефективності, робоче навантаження оновлення шифротексту надходить на сервер, використовуючи метод повторного шифрування проксі так, щоб новий користувач також міг розшифрувати дані, опубліковані до його входу у систему (зворотна безпека). Тим паче, що всі користувачі повинні тримати останній секретний ключ, а не вести записи про всі попередні секретні ключі.

Для реалізації детального контролю доступу спочатку власник поділяє дані на кілька компонентів та шифрує кожен компонент даних різним ключем за допомогою симетричних методів шифрування. Потім власник застосовує схему CP-ABE (схема шифрування кожного ключа) [13]. Користувачі з різними атрибутами можуть розшифрувати різну кількість ключів і у такий спосіб отримати різну інформацію у разі звернення до тих самих даних.

У системі є п'ять об'єктів (рис. 3): центр сертифікації ключів (ЦСК), атрибути доступу (АД), Власник, Хмарний сервер та Користувач. ЦСК налаштовує систему, реєструє всіх Користувачів, а також АД. Кожному Користувачу в системі ЦСК присвоює унікальний ідентифікатор користувача (uid), а також створює унікальний відкритий ключ для цього Користувача. Однак ЦСК не бере участі в управлінні атрибутами та створенні секретних ключів, пов'язаних з атрибутами. Наприклад, ЦСК може бути адміністрацією соціального захисту. Кожному користувачеві можна видати унікальний номер соціального страхування як глобальний ідентифікатор. Кожен АД відповідає за надання права на відкликання атрибутів користувачів (aid) відповідно до їх функцій. У запропонованій схемі кожен атрибут асоціюється з одним АД, але кожен АД може керувати довільною кількістю атрибутів. Також кожен АД має повний контроль над структурою і семантикою його атрибутів. Кожен АД відповідає за створення публічного ключа атрибутів для кожного його атрибуту та керує секретним ключем для кожного користувача.

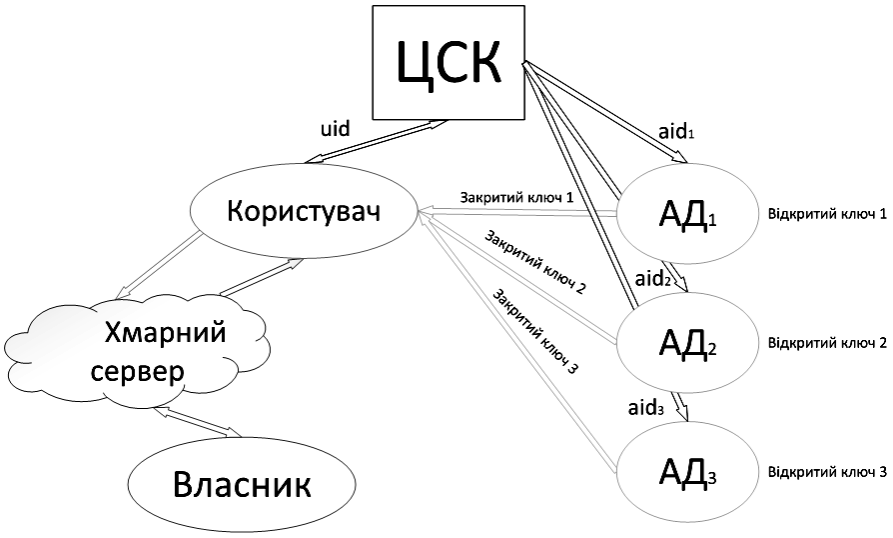

Рис. 3. Схема децентралізованого доступу до даних

Алгоритм роботи децентралізованого доступу ґрунтується на схемі доступу до даних CP-ABE:

1. Налаштування ЦСК. Він не приймає ніяких параметрів. Він генерує головний ключ, системний параметр і сертифікат.

2. Налаштування АД. Отримує від ЦСК aid. Генерує відкритий і закритий ключі, а також набір версійних ключів.

3. Шифрування. Запускає Власник даних, який отримує системний параметр і набір відкритих ключів для відповідного доступу до даних. Алгоритм шифрує відповідно до структури доступу і виводить шифротекст. Передбачається, що шифротекст неявно містить структуру доступу.

4. Генерація позначки шифрування. Запускає Хмарний сервер, отримує шифротекст від Власника даних і набір закритих і відкритих ключів.

5. Дешифрування. Запускає Користувач. Як вхідні дані беруть шифротекст, позначку розшифрування і глобальний закритий ключ Користувача.

Висновки

У роботі запропоновано вдосконаленння схеми контролю доступу CP-ABE для багато-користувацьких хмарних систем зберігання даних з ефективним дешифруванням та скасуванням операцій. Запропоновано результативний метод скасування атрибутів, який забезпечує зворотну безпеку. Схему децентралізованого доступу можна використовувати в приватних або гібридних хмарних системах зберігання даних.

Список літератури

1. Mell, P., & Grance, T. (2011, september). The NIST Defination of Cloud Computing. Gaithersburg, MD, United States. Retrieved September 2016, from http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

2. Dhar, S. (2012). From Outsourcing to Cloud Computing: Evolution of it Services. Management Research Review, 35(8), 664–675. 3.

3. Ogu, E. C., Alao, O., Omotunde, A., gbonna, A., & Izang, A. (2014). Partitioning of Resource Provisions for Cloud Computing Infrastructure against DoS and DDoS Attacks. International Journal of Advanced Research in Computer Science, V(7), 67-71. doi:10.13140/2.1.2259.7129.

4. Atchinson, Brian K.; Fox, Daniel M. (May–June 1997). "The Politics Of The Health Insurance Portability And Accountability Act" (PDF). Health Affairs. 16 (3): 146–150. doi:10.1377/hlthaff.16.3.146. Archived (PDF) from the original on 2014-01-16.

5. "What You Need to Know About PCI DSS Compliance: UK Costs & Checklist". Retrieved December 18, 2018.

6. "U. S. State Department – Policy – Directorate of Defense Trade Controls". Pmddtc.state.gov. Archived from the original on September 14, 2010. Retrieved July 8, 2010.

7. Presidency of the Council: "Compromise text. Several partial general approaches have been instrumental in converging views in Council on the proposal for a General Data Protection Regulation in its entirety. The text on the Regulation which the Presidency submits for approval as a General Approach appears in annex, "201 pages, 11 June 2015, PDF, http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf.

8. Atchinson, Brian K.; Fox, Daniel M. (May–June 1997). The Politics Of The Health Insurance Portability And Accountability Act. Health Affairs[en] 16 (3): 146–150. doi:10.1377/hlthaff.16.3.146.

9. 1McClennan, Jennifer P.; Schick, Vadim (2007). "O, Privacy: Canada's Importance in the Development of the International Data Privacy Regime". Georgetown Journal of International Law. 38: 669–693.

10. Lewko A. B. and Waters B. "Decentralizing attribute-based encryption," in EUROCRYPT'11. Springer, 2011, pp. 568–588.

11. Xiaoyun Wang, Dengguo Feng, Xuejia Lai, Hongbo Yu: Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD, Cryptology ePrint Archive Report 2004/199, 16 Aug 2004, revised 17 Aug 2004. Retrieved July 27, 2008.

12. Green, M., Hohenberger, S., Waters, B. Outsourcing the decryption of ABE ciphertexts. In: Proceedings of the 20th USENIX Security Symposium. USENIX Association (2011). 13. M. Chase, "Multi-authority attribute based encryption," in TCC'07. Springer, 2007, pp. 515–534.

DECENTRALIZED ACCESS MANAGEMENT SCHEME TO THE CLOUD DATA STORAGE

L. Berezko, V. Tatianchuk

Lviv Polytechnic National University,
Department of Electronic Computers

Consideration is given to enhancing storage security and maintaining data access control in cloud storage. Existing ways of controlling such access are analyzed. An enhancement of the encryption technique is proposed, based on the attributes of the ciphertext policy and its application in a decentralized data access management system in multi-user cloud storage systems. The main objective is to improve the security and privacy of the management of the cloud storage for which the existing management does not meet all the necessary requirements.

Key words: cloud data warehouses, access, encryption.