**УДК** [**004.65**](https://teacode.com/online/udc/00/004.65.html)**, 004.62**

**Тат’янчук В.П., Березко Л.О.**

Національний університет "Львівська політехніка"

кафедра електронних обчислювальних машин

**Використання платформ захищених хмарних обчислень для побудови сховищ даних**

*© Тат’янчук В.П., Березко Л.О., 2019*

**Розглянуто проблеми безпеки та конфіденційності при доступі до даних у хмарних сховищах даних. Проаналізовані способи контролю доступу до даних у хмарі. Запропоновано підхід до вдосконалення техніки** **шифрування на основі атрибутів політики шифротексту у децентралізованій системі контролю доступу до даних для багатокористувацьких хмарних систем зберігання даних. Основною метою є підвищення безпеки та конфіденційності для хмарного сховища даних до якого існуючий доступ управління не відповідає всім вимогам безпеки та конфіденційності.**

**Ключові слова: шифрування, хмарні обчислення, сховища даних.**

**Security and privacy issues when accessing data in cloud storage are discussed. Ways to control access to data in the cloud are analyzed. An approach to improving encryption techniques based on the attributes of the ciphertext policy in a decentralized data access control system for multi-user cloud storage systems is proposed. The primary objective is to enhance security and privacy for the cloud storage to which existing management access does not meet all security and privacy requirements.**

**Keywords: encryption, cloud computing, data warehouses.**

**Вступ.** Національний інститут стандартів та технологій [1] визначив хмарні обчислення як "модель для забезпечення зручного доступу до мережі за запитом до спільного пулу налаштованих обчислювальних ресурсів (наприклад, мереж, серверів, зберігання, додатків та послуг), що швидко розробляються та звільняється з мінімальними зусиллями управління або втручання постачальника послуг ». Він має кілька моделей розгортання, які є публічними, приватними та гібридними хмарами [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]. Не так давно у Європі був прийнятий досить обтяжливий закон General Data Protection Regulation (GDPR) з його широкими правилами та жорсткими штрафами для всії країн Європейського Союзу (ЄС), які диктують, що конфіденційна або приватна інформація повинна знаходитиися у фізичних межах країни чи регіону з якої вони походять [8]. Є також Закон Великобританії про захист даних, Федеральний закон Швейцарії про захист даних та Канадський Personal Information Protection and Electronic Documents Act (PIPEDA)[9]. Таким чином ми маємо багато різних законів про безпеку та конфеденційність даних яких потрібно притримуватися у розробці хмарної інфраструктури.

У послугах хмарних обчислень клієнти стурбовані переміщенням своїх конфіденційних даних і додатків зі своїх приватних обчислювальних середовищ в хмарну середовище, яка спільно використовується різними клієнтами і яке зазвичай доступне через загальнодоступну мережу. Несанкціонований доступ до інтерфейсу управління: в хмарних обчисленнях інтерфейси управління зазвичай доступні через загальнодоступні мережі для авторизованих клієнтів і можливих неавторизованих зловмисників, тоді як звичайні центри обробки даних зазвичай доступні тільки авторизованим адміністраторам безпосередньо або через приватні мережі. Більш того, доступ до управління зазвичай здійснюється через веб-додаток або сервісні технології, тому інтерфейс управління хмарами, ймовірно, схильний до вразливості цих технологій.



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

**Стан проблеми.** Поняття безпеки та конфіденційності інформації в хмарі є критичною проблемою. Це може бути пов'язано з тим, що в Хмарах немає меж, і дані, що зберігаються в хмарі, можуть бути фізично розміщені в будь-якій точці світу або в будь-якому центрі обробки даних в мережі, що географічно розподіляється, як це передбачено Cloud Security Group [4]. Іншими словами, Хмарні бази даних викликають серйозні проблеми безпеки, такі як доступність, конфіденційність, приватність, цілісність даних та цілісність інформації, серед інших, які мають найважливіше значення. Тому слід пропонувати рішення для вирішення всіх цих питань, зокрема конфіденційності та цілісності даних у хмарній базі даних, для зберігання, доступу, маніпуляцій та взаємодії з користувачами та серед них. Яскравий характер бази даних Хмари зробив її дуже вразливою до декількох атак безпеки, конфіденційності та етичних проблем. Більшість етичних питань, пов’язаних із хмарою, стосуються питань довіри та недовіри між постачальниками послуг Cloud та абонентами Cloud. Дослідження рекомендує стратегії або способи, за допомогою яких такі проблеми можна пом'якшити, запропонувавши систему безпеки та конфіденційності. Велика кількість законів про конфіденційність, змусила багато компаній відмовитися від зберігання даних у хмарі, тому що хмарні платформи не можуть гаратнтувати безпеку даних користувачів. Багато провайдерів можуть зберігати дані на серверах, які фізично не знаходяться в регіоні, що суперечить законам деяких країн. Це проблема для фірм, що мають чітке законодавство про зберігання даних.

Служба хмарного зберігання даних дозволяє власнику даних передавати свої дані в хмару і через неї забезпечує доступ до даних користувачеві. Тому що хмарний сервер і власник даних не в одному довірчому домені, у напівдовіреному хмарному сервері не можна покладатися на застосування політики доступу. Вирішують цю проблему зазвичай примшуючи власника даних шифровувати дані та надавати ключі шифрування авторизованим користувачам. Однак ці методи зазвичай включають складний ключ та великі накладні витрати власника даних. Тому питання безпеки та конфіденційності при доступі до даних у хмарних сховищах даних є актуальним.

**Постановка задачі.** Пропонується підхід до вдосконалення техніки шифрування на основі атрибутів політики шифротексту для контролю доступу до зашифрованих даних, який є не оптимальним для хмарних платформ і накладає обмеження по продуктивності тому запропонавоно децентралізовану схему доступу до даних.

**Розв’язок задачі.** Існуюча схема доступу до даних CP-ABE [10] запропонована Левком та Уотерсом має високий рівень безпеки і надійсності вона все ще не може бути застосована для контролю доступу для багатокористувацьких хмарних систем зберігання даних через неефективність дешифрування та скасування операції. З метою розробки ефективної схеми контролю ми візьмемо схему CP-ABE з ефективним розшифруванням та запропонуєм нлвий метод анулювання операції.

Важким питанням в розробці схеми CP-ABE з кількома повноваженнями - це як зв'язати секретні ключі разом і запобігти колізійним атакам[11]. Без центрального керування важко пов'язати разом різні компоненти секретного ключа користувача та використовувати ключовий метод рандомізації для запобігання колізыйних атак. В нашому методі, ми відокремлюємо повноваження на глобальний центр сертифікації ключів (ЦСК) та атрибути доступу (AД). CД налаштовує систему і приймає реєстрацію всіх користувачів та АД в системі. Однак ЦСК не бере участь в будь-якому управлінні атрибутами та створенні секретних ключів які пов'язані з атрибутами. ЦСК призначає глобальний ідентифікатор користувача, що відповідає індивідуальному користувачеві, та ідентифікатор глобального авторитету

допомога кожному атрибутивному органу в системі. Тепер він є унікальним у глобальній у системі, секретні ключі, видані різними AД для одного і того ж унікального ідентифікатора можуть бути пов'язані разом для дешифрування.

Оскільки кожен AД пов'язаний за допомогою ідентифікатора, ми можемо протистояти колізійним атакам[12].

Для досягнення ефективного розшифрування користувача, пропонуэться метод аутсорсингу на основі токена. Застосовуэться дешифрування ідеї аутсорсингу [13] та розширення її на кілька авторитетних систем, дозволяючи ЦСК генерувати глобальну пару секретного ключу та глобального відкритиго ключу для кожного користувача в система.

Під час дешифрування користувач подає свої секретні ключі Видані AД на сервер і просить сервер обчислити a токен дешифрування для розшифровки шифротексту. Потім користувач може розшифрувати шифротекст, використовуючи токен дешифрування разом із його глобальним секретним ключем.

Щоб вирішити проблему анулювання атрибута, ми присвоюємо кожному атрибуту номер версії. Щоб коли трапляється скасування атрибуту, лише ті компоненти які пов'язані з Анульованим атрибутом у секретних ключах та шифротекстах були оновлені. Коли атрибут користувача відкликається з будь-якого АД, AД генерує новий номер версії та генерує декілька ключів оновлення користувача та ключ оновлення шифротексту. Тому що ключі оновлення відрізняються для різних користувачів, відкликаний користувач не може оновити свій секретний ключ, використовуючи ключі оновлення інших користувачів (Зворотня безпека). Використовуючи ключ оновлення шифротексту, компонент, пов'язаний з відкликаним у шифротексті, може оновитися до поточної версії. Щоб підвищити ефективність, робоче навантаження оновлення шифротексту йде на сервер використовуючи метод повторного шифрування проксі, таким чином, щоб новий користувач також може розшифрувати попередні опубліковані дані, які публікувалися до його вступу в систему (Зворотня безпека).Більше того, всі користувачі повинні тримати останній секретний ключ а не вести записи про всі попередні секретні ключі. Щоб реалізувати детальний контроль доступу, спочатку власник розділяє дані на кілька компонентів та шифрує кожен компонент даних різні ключем вмісту за допомогою симетричних методів шифрування.Потім власник застосовує схему CP-ABE(схема шифрування кожного ключа). Користувачі з різними атрибутами можуть розшифрувати різну кількість ключів вмісту і таким чином отримати різну інформацію з одних і тих же даних.



Рис. 2. Схема децентралізованого доступу до даних.

У системі є п'ять об'єктів, як показано на рис. 2, центр сертифікації ключів (ЦСК), атрибути доступу (AД), влассник, хмарний сервер та користувач. ЦСК налаштовує систему, а також приймає реєстрацію всіх користувачів, а також АД в системі. Кожному користувачеві в системі ЦСЛ присвоює йому унікальну ідентифікатор користувача, а також створює унікальний відкритий ключ для цього користувача. Однак ЦСК не приймає участь в управлінні атрибутами та створенні секретних ключів, пов'язаних з атрибутами. Наприклад, ЦСК може бути адміністрацією соціального захисту. Кожному користувачеві може бути виданий унікальний номер соціального страхування в якості глобального ідентифікатора. Кожен AД відповідає за надання права та відкликання атрибутів користувачів відповідно до їх ролі. У запропонованій схемі кожен атрибут асоціюється з одним AД, але кожен АД може керувати довільною кількістю атрибутів. І кожен АД має повний контроль над структурою і семантикою його атрибутів. Кожен AД відповідає за створення публічного ключа атрибутів для кожного його атрибуту та керує секретним ключем для кожного користувача.

**Висновки.** У роботі було запропоновано ефективну схему контролю доступу до даних для багатокористувацьких хмарних систем зберігання даних. Також було побудовано нову схемму шифрування на основі атрибутів політики шифротексту, в якій основне обчислення дешифрування передаються на сервер. Ця схема може застосуватися в системах хмарного зберігання даних.

**Література**

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. A. B. Lewko and B. Waters, “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. M. Chase, “Multi-authority attribute based encryption,” in TCC’07. Springer, 2007, pp. 515–534.
13. K. Yang, X. Jia, and K. Ren, “Dac-macs: Effective data access control for multi-authority cloud storage systems,” IACR Cryptology ePrint Archive, vol. 419, pp. 1–12, 2012.