УДК 621.39

ВИКОРИСТАННЯ АУТЕНТИФІКАЦІЇ В МЕРЕЖІ ЯК СПОСОБУ ВИКОНАННЯ БЕЗПЕЧНИХ ХМАРНИХ ОБЧИСЛЕНЬ

Григоренко О.Г., Полікарпова Ю.Г.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: olenagri@ukr.net, july.polik@gmail.com

NETWORK AUTHENTICATION USING AS A WAY TO PERFORM SECURE CLOUD COMPUTING

The main authentication methods in the network are analysed, this allow to use cloud storage and perform cloud computing safely with the growing potential threats of data theft of organizations.

Проаналізовані основні методи аутентифікації в мережі, що дозволяють безпечно використовувати хмарні сховища та виконувати хмарні обчислення при зростанні потенційних загроз крадіжок даних організацій

Процес аутентифікації в мережі служить захистом від різного роду атак, метою яких є крадіжка даних у хмарному середовищі. Хмарні обчислення здебільшого використовуються різними організаціями в багатьох комерційних сферах. Постачальники хмарних послуг відповідають за ідентифікацію та інші види управління в хмарному середовищі. Однак велика кількість випадків витоку даних спричинена вразливістю в системах управління ідентифікацією. Методи аутентифікації підтверджують ідентифікацію користувача перед тим, як дати дозвіл на доступ до ресурсів. Процес аутентифікації зазвичай виконується програмним забезпеченням або його частиною. Приклад процесу аутентифікації показаний на рис.1. Хмарна система виконує один або поєднання зазначених нижче методів аутентифікації.

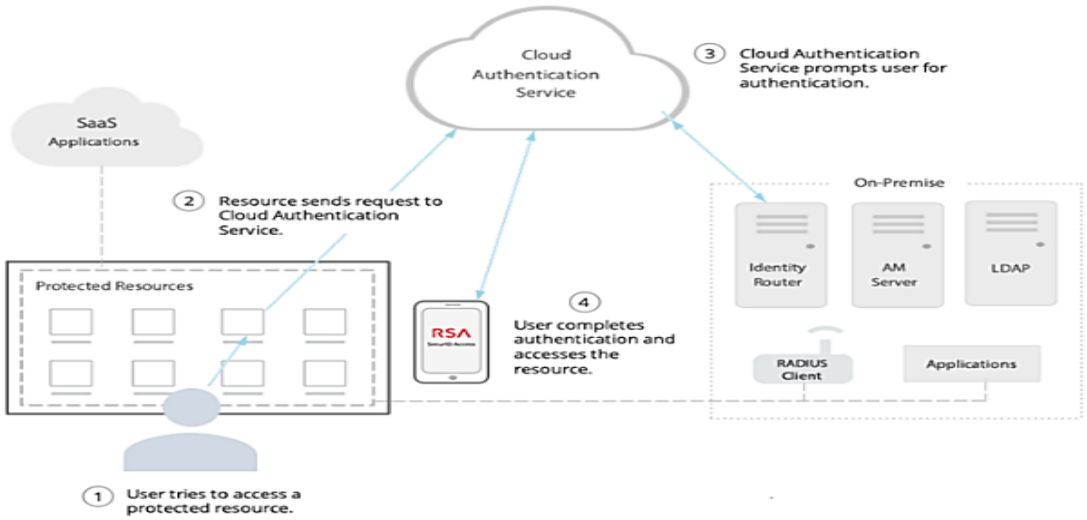

Рис.1. Приклад процесу аутентифікації в хмарному середовищі [4].

Картки доступу та біометрична аутентифікація: розпізнавання райдужки або сітківки ока, розпізнавання відбитків пальців, розпізнавання обличчя та розпізнавання долоні, забезпечують безпеку хмарних ресурсів та засобів, забороняючи несанкціонований доступ. Хмарні центри обробки даних (Cloud data centers - CDC) концентрують усі сервери, мережі та програми, щоб користувачі мали доступ до даних у будь-який час і з будь-якого місця. Для запобігання витоку даних з боку інсайдерів або будь-якого несанкціонованого доступу до CDC фізична безпека необхідна разом із певними політиками використання та управління.

Для виконання безпечних хмарних обчислень важливими є ідентифікаційні дані, які підтверджують повноваження, статус, права та права доступу. Використання таких облікових даних, як одноразовий пароль, шаблон та капча, є традиційним способом захисту системи від зловмисних дій. Найбільш часто використовуваними механізмами управління обліковими даними доступу для хмарного середовища є технології Lightweight Directory Access Protocol (LDAP) та Microsoft Active Directory (AD). Серверами LDAP та AD керують сторонні постачальники або в рамках організаційної мережі хмарних обчислень. Витрати на хмарне обслуговування збільшуються, коли на цих традиційних механізмах управління обліковими даними розгортається кілька програм. Дуже важливо додавати, вимикати, змінювати або видаляти облікові записи кожного разу, коли працівник виходить або входить в організацію. При управлінні обліковими даними на стороні провайдера виникає вразливість скидання облікових даних, коли використовуються слабкі механізми відновлення пароля. Хакери можуть відслідковувати, обробляти або компрометувати облікові дані. Ключі захищеної оболонки (Secure Shell keys - SSH) допомагають ідентифікувати сервер SSH за допомогою криптографії з відкритим ключем або аутентифікації виклику-відповіді. Головною перевагою ключів SSH є те, що аутентифікація на сервері виконується без передачі пароля по мережі. Це запобігає перехопленню або зламу пароля хакерами. Спроби вгадати облікові дані за допомогою атак грубої сили усуваються ключами SSH. Агенти SSH допомагають встановити зв’язок із серверами без використання окремих паролів для кожної системи. Агент SSH зберігає приватні ключі та надає їх клієнтським програмам SSH. Ці приватні ключі зашифровані парольною фразою, яка надається під час кожної спроби з'єднання з сервером. У кожному окремому виклику SSH парольні фрази необхідні для дешифрування приватного ключа перед тим, як перейти до фази аутентифікації. Парольна фраза використовується лише під час додавання приватних ключів до сховища агента. Основна проблема ключів SSH полягає в тому, що ключі можуть бути недостатньо захищені. Ідентифікаційні дані та ключові механізми SSH зазвичай використовуються для аутентифікації хмарних веб-служб [1].

Багатофакторна аутентифікація – ще один метод захисту цифрових активів та транзакцій через Інтернет. Як правило, одноразові паролі (One-Time Password - OTP), капчі або шаблони використовуються як вторинний механізм аутентифікації разом із ідентифікаційними даними. Багатофакторність забезпечує додатковий рівень безпеки над традиційною аутентифікацією на основі ідентифікаційних

даних. Як правило, онлайн-транзакції аутентифікуються за допомогою одноразових паролів. При фінансових операціях через Інтернет сервер за певними алгоритмами генерує одноразовий пароль, який надсилається користувачеві або через зареєстрований номер мобільного телефону, або електронною поштою. Інший тип OTP генерується за допомогою апаратних/програмних генераторів маркерів, який захищений персональним ідентифікаційним номером (PIN). Цей пароль можна використовувати один раз, і він має певний термін використання. Капчі зазвичай використовується для захисту веб-програм від атак зловмисного програмного забезпечення. Капча може бути буквенно-цифровою комбінацією, математичним рівнянням або зображенням. [2]

Безпека механізмів чіпа та PIN-коду полягає у використанні відкритих та приватних ключі для асиметричного шифрування та дешифрування даних. Мікропроцесорний чіп зберігає дані користувача та ключі безпеки шляхом створення унікальних даних про фінансові транзакції для захисту від шахрайства [1,3]. Зв'язок між клієнтом/терміналом із сервером аутентифікації шифрується та підписується за допомогою ключа безпеки, який зберігається в мікросхемі. Сервер перевіряє підпис і розшифровує зв'язок за допомогою ідентичних ключів, які зберігаються на сервері. PIN-код використовується для аутентифікації клієнта/терміналу для доступу до даних.

Метод єдиного входу (Single Sign-On-SSO) допомагає хмарним користувачам використовувати один пароль для доступу до всіх додатків/послуг, зберігаючи по одному обліковому запису для кожного користувача. Користувачам не потрібно вказувати свої облікові дані під час кожного доступу до різних хмарних веб-служб.

Підсумовуючи, зазначимо, що найбільш цінним ресурсом в хмарних обчисленнях є дані користувачів. Захист даних користувача вкрай важливий і значущий. Тому рішення щодо безпеки в цій системі постійно оновлюються. Важливою частиною безпеки даних у хмарі є аутентифікація. Проаналізовані методи біометричної, багатофакторної аутентифікації, використання ідентифікаційних даних, ключів SSH, механізмів чіпа та PIN-коду, методу єдиного входу дозволяють різним організаціям в багатьох комерційних сферах безпечно використовувати хмарні сховища та безпечно виконувати хмарні обчислення.

Література

1. ISSN: 2277 128X: International Journal of Advanced Research in Computer Science and Software Engineering/ [Електронний ресурс] – Режим доступу: http://www.ijarcsse.com/.
2. Воронцов А. В., Газизова Э.Р., Веденьев Л.Т., Афанасьев А. Н. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. –Учебное пособие для вузов, – 2009 г., 278 – 301 с.
3. Бердник А. Угрозы облачных вычислений и методы их защиты [Електронний ресурс] / Алексей Бердник. – 2013. – Режим доступу до ресурсу: https://habr.com/ru/post/183168/.
4. RSA SecurID® Access Cloud Authentication Service Documentation/ [Електронний ресурс] – Режим доступу: https://community.rsa.com/t5/rsa-securid-access-cloud/cloud-authentication-service-overview/ta-p/569175.