Технічні науки

УДК 044

Шепшелей Аліна Володимирівна
студент
Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»
Шепшелей Алина Владимировна
студент
Национального технического университета Украины
«Киевский политехнический институт имени Игоря Сикорского»
Shepshelei Alina
Student of the
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute"

Пасько Віктор Петрович
кандидат технічних наук, доцент кафедри технічної кібернетики
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Пасько Виктор Петрович
кандидат технических наук, доцент кафедры технической кибернетики
Национальный технический университет Украины
«Киевский политехнический институт имени Игоря Сикорского»
Pasko Viktor
PhD, Asociate Professor at Technical Cybernetic Department
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute"

Застосування гомоморфних систем криптографічного захисту інформації в хмарних обчисленнях

Анотація. *Досліджено доцільність та необхідність застосування гомоморфних систем криптографічного захисту інформації в хмарних обчисленнях.*

Ключові слова: *криптосистема, хмарні обчислення, шифрування, безпека даних.*

Аннотация. *Было исследовано необходимость и возможность применения гомоморфных систем криптографической защиты информации в облачных вычислениях.*

Ключевые слова: *криптосистема, облачные вычисления, шифрование, безопасность данных.*

Summary. *The expediency and necessity of using homomorphic cryptographic information security systems in cloud computing.*

Key words: *cryptosystem, cloud computing, encryption, data security.*

Починаючи з 2008-го року термін «хмарні обчислення» почав активно поширюватися по світу. Основною ідеєю хмарних техноголій є надання ресурсів за вимогою. Тим самим суб'єкту, який орендує ресурси, немає необхідності утримувати ці ресурси.

Концепція хмарних обчислень є ринковою відповіддю на посилення ролі аутсорсингу в IT-індустрії. Перехід на хмарні технології означає передачу на аутсорсинг традиційних процесів управління IT-інфраструктурою зовнішнім професійним підрядникам.

Використання технології хмарних обчислень дає багато переваг, але для роботи з даними у публічній хмарі є необхідність працювати з відкритими даними. Для роботи з конфіденційними даними така схема роботи неприйнятна, так як, дані не зашифровані і досить легко можна отримати до них доступ. Є необхідність застосовувати оранізаційні міри для збереження ключів і закупляти апаратуру для посиленого контролю доступу

та шифрування інформації. Ставити ультиматуми щодо підвищення безпеки перед провайдером хмар немає сенсу, бо вони відразу себе обмежують у відповідальність за доступ третьої сторони до ваших даних. Ідеальнобезпечною виглядає алгоритм, коли дані передаються у зашифрованому вигляді, а подальші операції з даними ніяким чином не розшифовували їх. Для реалізації цього задуму ми можемо використати гомоморфні системи шифрування [4].

Гомоморфне шифрування – це тип шифрування, коли ми маємо можливість працювати напряму з зашифрованими даними: виконувати певні математичні дії і отримувати зашифрований результат, що є результатом відповідної операції з розшифрованим текстом.

Криптосистема RSA є однією з найвідоміших та найпопулярніших криптосистем. Ця криптосистема є гомоморфною щодо операції множення. Опис схеми було опуліковано у 1977 році Рональдом Райвестом, Аді Шаміром та Леонардом Адлеменом у стінах Масачусетського Технологічного Інституту. RSA формується з 4 етапів операцій:

- Генерація ключів;
- Шифрування;
- Розшифрування;
- Розповсюдження ключів.

Безпеку використання заберзпечує принцип факторизації цілих чисел. Алгоритм є асиметричним, тому використовуються два ключі: приватний та публічний [1].

Криптосистема Гентрі – це перша вдала спроба реалізувати криптосистему, яка буде гомоморфною, як за операцією додавання, так і множення. Схема базується на використанні ідеальних граток. Вперше вода була запропонована в 2009 році, в рамка докторської дисертації Крейга Гентрі. Так, як система гомоморфна за двома операціями, то стає можливим реалізувати алгоритми, для будь-яких довільних обчислень.

Для практичної реалізації схеми використовуються наступні операції: генерація ключів, шифрування, розшифрування та оцінка [1].

Дохід від хмарних обчислень задежить від якості послуг, які пропонує хмарний постачальник послуг. Основним атрибутом якості сервісу є безпека, а постачальник хмарних сервісів повинен забезпечити повну гарантію безпеки з точки зору конфіденційності, доступності та цілісності. Серед усіх факторів конфіденційність є основним та незламним фактором безпеки. Шифрування – це спосіб захистити дані, які розміщені на ненадійному хмарному сервері. Більшість алгоритмів, які зараз доступні не мають впливу на додатки в реальному часі. Можливість їх використання в критичному обладнанні обмежена. Таким чином, ми класифікуємо різні алгоритми шифрування на основі їх зручності та адаптивності. Використовуючи шифрування на основі атрибутів (ABE). На відмінну від інших методів шифрування ABE займається шифруванням та дешифруванням даних на основі атрибутів користувача. Це забезпечує багатообіцяючий та гнучкий контроль доступу за допомогою керованих структур доступу, пов'язаних із приватним ключем, основним ключем та текстом шифру. Шифрування на основі атрибутів – це чудовий спосіб захиститись від інших типів шифрування, таких, як роль на основі доступу, оскільки вона має можливість обмежувати доступ на основі ролей. У результаті це підходить лише для невеликих додатків. ABE є накладними з точки зору пошуку даних. З огляду на фактори конфіденційності та безпеки обмеження незначні [2].

У хмарних обчисленнях дані зберігаються в невідомому для кінцевого користувача місці. По-перше, дані повинні бути захищені в базі даних. Віртуалізація забезпечує рішення для захисту даних. Для досягнення безпеки та цілісності місця зберігання таємниці. Питання полягає в тому чи слід вірити в ненадійний хмарний сервер. Ми заявили, що це не довіряє, оскільки воно включає в себе багато шкідливих атак під час обробки даних. ABE пропонує складний механізм контролю доступу над зашифрованими даними.

В основному, ABE – це відкритий ключ, що заснований на одному шифруванні, який розшифровує текст шифру, лише в тому випадку, коли приватний ключ, який пов'язаний з користувачем, співпадає з відкритим ключем та основним секретним ключем. Дешифрування відбувається безпосередньо самим сервером. Тим самим продуктивність збільшується за допомогою ефективних методів шифрування. Вона страждає від серйозних недоліків розшифровки. Структура доступу надає повний доступ до користувача. Це є основним обмеженням шифрування на основі основних атрибутів. Повний доступ наданий користувачеві створює багато проблем. KP-ABE не в змозі відрізнити необхідний контроль доступу користувачам, як політику доступу, вбудовану в ключ розшифровки [3].

Як було описано раніше, сьогодні для забезпечення безпеки хмарних обчислень використовується алгоритм KP-ABE, який містить наступні недоілки:

- Можливе накопичення атрибутів, які не мають відношення до даних і таким чином збільшення розміру шифротексту;
- Продуктивність ситеми лінійно залежить від кількості користувачів;
- Якщо ключ доступу користувача підійте дані будуть розшифровані на сервері, що небезпечно для публічних хмар;
- На машині користувача, з якої відбувається підключення до хмари, повинен бути встановлений ключ, що знову ж впливає на безпеку. В такому випадку під час атаки на хмару може бути отриманий доступ і до пристрою користувача [4].

Якщо ж ми будемо використовувати повністю гомоморфні системи або частково гомоморфні системи, то отримуємо ряд переваг за рахунок незначних жертв у часі роботи, а саме:

- Ми працюємло лише з безпосередньо необхідними даними і не застосовуємо зайвих параметрів;

- Для систем можлива реалізація розпаралелювання процесів шифрування та розшифрування;
- Жодна інформація не буде розшифрована на сервері, лише безпосереднім користувачем у довіреній зоні;
- Можна здійснювати операції додавання та множення із зашифрованими даними, без попереднього розшифрування;
- Усі здійснені з зашифрованим текстом операції ніяким чином не позначаються на процесі розшифрування.

Криптостійкість частково та повністю гомоморфних систем достатня, для того, щоб виключити атаку методом повного перебору. Для алгоритму RSA застосовується факторизація цілих чисел, що виключає і додатково, алгоритм є асиметричним. Саме сукупність цих факторів надає достатню криптостійкість алгоритму. Для моделі Бракерські-Гентрі-Верткаутенер також актуальна ознака асиметричності алгоритму, який використувється у системі та додатковим фактором, що сприяє підвищенню криптостійкості - це використання ідеальних граток. Ці фактори також забезпечують достатню криптостійкість алгоритму перед зловмисниками [1].

Попри усі позитивні якості обидві криптосистеми мають суттжві недоліки:

- Відносно не висока продуктивність роботи для одного шифротексту;
- Для повністю гомоморфних систем спостерігається накопичення помилки, що після певної межі впливає на коректність результатів;
- Алгоритми чутливі до величини ключа шифротексту, тому необхідно обробляти інформацію лише невеликими пакетами.

Література

1. Ільєнко А. В. Забезпечення конфіденційності інформаційних ресурсів на основі методів гомоморфного шифрування / А. В. Ільєнко, Р. В.

Зюбіна // Авіа-2015: XII міжнародна науково-технічна конференції, 28-29 квітня 2015 р.: тези доп. – К., 2015. – С. 5.25-5.29.

2. Н. П. Варновский. Гомоморфное шифрование [Електронний ресурс] / Варновский Н. П. , Шокуров А. В // РФФИ. – 2011. – №6. – С. 27 – 36.
3. Иванов М. А. Криптографические методы защиты информации в компьютерных системах и сетях / М. А. Иванов. – Москва: Кудиц – Образ, 2007. – 368 с.
4. NIST Определение облачных вычислений [Електронний ресурс]. – Режим доступу: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf