УДК 004.056.5(045) **Корнієнко Б.Я., Юдін О.К., Снігур О.С.**

БЕЗПЕКА АУТЕНТИФІКАЦІЇ У WEB-РЕСУРСАХ

У даній статті проаналізовано основи концепції Cloud Computing, визначено основні переваги та вразливості концепції. Розглянуто аутентифікацію користувачів в концепції Cloud Computing та основні можливості для спрощеного управління безпекою.

Ключові слова: Cloud Computing, безпека, вразливість, аутентифікація, загроза.

*Вступ***.** Cloud Computing - це давня мрія постачати обчислювальні потужності, як послуги. Концепція Cloud Computing має потенціал трансформувати велику частину IT-індустрії, зробивши програмне забезпечення більш доступним та привабливим, надаючи його як сервіс та змінивши спосіб постачання апаратних ресурсів. Новатори, що мають свіжі та нові ідеї для створення Інтернет-сервісів зможуть зосередитись на створенні та розробці сервісу і приділяти значно менше уваги його технічному забезпеченню та підтримці. Користувачі концепції зможуть отримувати обчислювальні потужності саме в тому обсязі, в якому потрібно для роботи їх систем, тим самим уникнувши проблем перевикористання або браку ресурсів, що сприяє прямій економічній вигоді. Крім того, користувачі, що мають потребу оброблювати велику кількість запитів, отримають змогу обробляти інформацію набагато швидше, оскільки використання 1000 серверів протягом 1 години еквівалентно використанню 1 сервера протягом 1000 годин. Така гнучкість ресурсів та їхня необмежена потужність дають змогу вважати, що дана концепція може бути актуальною та перспективною.

Аналіз існуючих досліджень та постановка проблеми. Концепція Cloud Computing є новою та потребує детального вивчення, дослідження шляхів її застосування та інтеграції її в інші системи. У зарубіжних дослідженнях концепції Cloud Computing одержані вагомі результати, але питанню використання концепції Cloud Computing в побудові систем захисту комп'ютерних мереж, приділяється досить мало уваги. Cloud Computing може бути ефективним інструментом для створення систем аналізу даних в системах виявлення вторгнень, що на сьогодні є досить актуальним питанням. Таким чином, **метою даної статті** є дослідження проблем безпеки web-ресурсів та використання механізму автентифікації у Cloud Computing.

*Визначення Cloud Computing***.** Термін Cloud Computing тісно пов'язаний з новою парадигмою, що стосується забезпечення обчислювальною інфраструктурою комп'ютерні мережі. В основі цієї парадигми лежить спроба перенести інфраструктуру в мережу, тим самим знизити видатки, що пов'язані з підтримкою та управління апаратними та програмними засобам. Cloud Computing привернув до себе увагу IT спільноти завдяки тому, що останнім часом з'явилось багато сервісів, що мають спільні характеристики та представлені основними гравцями ринку IT (наприклад Google Appengine, Amazon EC3)[1]. Але, слід зауважити, що деякі технології на яких ґрунтується концепція CloudComputing (наприклад візуалізація, кластерні обчислення або розподілені обчислення) не нові. Cloud Computing – це необмежена кількість віртуалізованих, ресурсів (таких як апаратні, програмні платформи та інші послуги), які можуть бути динамічно розподілені, щоб забезпечувати роботу при максимальному навантаженні та надаються за моделлю плата-за-використане, а якість послуг гарантована угодою SLA.

*Типи Cloud Computing***.** Існує декілька видів діяльності пов'язаних з Cloud Computing: *Постачальники Послуг* (ПП) роблять свої послуги доступними через Інтернет для *Користувачів Послуг* (КП). Метою CloudComputing є аутсорсинг забезпечення обчислювальної інфраструктури, яка необхідна для розміщення цих послуг. Інфраструктура пропонується «як сервіс» *Постачальниками Інфраструктури* (ПІ), переносячи тим самим інфраструктуру від ПП до ПІ, в результаті ПП можуть отримати гнучкість своїх рішень та зменшити видатки на їх обслуговування.

Слід більш детально розглянути кожний з типів CloudComputing:

- Інфраструктура як послуга (IaaS)

IaaS є важливим альтернативним центром обробки даних ресурсів, таких як місце для зберігання, фізичні сервери, комутатори, брандмауери та маршрутизатори зі значно більшими ресурсами в хмарі. Основні постачальників IaaS на ринку: Amazon, IBM тендери, 42U центр обробки даних, оснащений попередньо встановленим і налаштованим апаратними засобами GoGrid та FlexiScale.

- Платформа як послуга (PaaS)

PaaS іноді називають "cloudware", так як це переміщеняя ресурсів з машини користувача в хмару. PaaS є моделлю для переміщення операційних систем і послуг в Інтернет без завантаження. Його постачальниками є Coghead, Google (Google App Engine) salesforce.com (Force.com), iDapper.net.

- Програмне забезпечення як послуга (SaaS)

SaaS є програмним продуктом, в якому програми розміщуються для продавця або постачальника послуг і ці програми доступні для використання через Інтернет. До SaaS належать salesforce.com, CRM-програми, ERP-програми, Citrix, служби Google, що включають в себе Gmail, Google Docs, Google Talk та інші.

Переваги Cloud Computing. Три рівня сервісів (SaaS, IaaS, PaaS) співпрацюють один з одним у хмарі, що чудово зменшує витрати ресурсів. Групування ресурсів також призводить до більш високої продуктивності, стеку гармонізації (компетентний контроль навантаження) та повне використання потенціалу серверу. З цієї точки зору обчислювальна хмара є неперевершена в обслуговуванні та розширювана у використанні ресурсів.

Основні переваги Cloud Computing: Cloud computing надає більш ефективну безпеку в центральній базі доступу, крім того, забезпечує використання автоматизованих систем інтерфейсів. Користувачеві не потрібно піклуватися про технічне обслуговування та усунення несправностей поточних операцій; Використання Cloud computing по всьому світу за допомогою новітніх технологій; Використання клієнтами Cloud computing, доступ до середовищ і послуг які утримуються третьою стороною. Тобто кожен може отримати доступ по всьому світу з будь-якої утиліти та в будь який час з портативного пристрою, ПК та ноутбуку.

*Вразливості Cloud Computing***.** Розглянемо основні вразливості Cloud Computing[2].

Вразливості служби забезпечення. Основними факторами впливу на службу забезпечення можуть бути:

- Відсутність контролю забезпечення клієнтом
- Копіювання ідентифікаційних даних
- Затримка синхронізації компонентів Cloud Computing
- Невірна ідентифікація клієнта при авторизації

Вразливості аутентифікації. Cloud Computing використовують дворівневу модель доступу до ресурсів, так як всі програми доступні в Інтернеті. Факторами, що впливають на несанкціонований доступ до ресурсів можуть бути:

- Помилки та вразливості в привілеях
- Зберігання облікових даних на тимчасових машинах
- Неправомірне використання клієнтом даних Cloud Computing

Вразливості гіпервізора. Дана атака є досить популярною, так як атаки даного типу мають змогу контролювати розподіл даних між віртуальною машиною та клієнтом. Гіпервізор має змогу контролювати розподіл ресурсів, що може бути критичним для системи в цілому. *Вразливості шифрування.* Дані вразливості призводять до атак типу зчитування даних під час передачі ресурсів. Як приклад можна навести атаки типу MITM. *Вразливості процедури управління ключами.* Cloud Computing використовує різні види ключів, а саме: сеансові ключі, ключові пари для ідентифікації провайдерів та клієнтів, ключі шифрування файлів. Cloud Computing має територіально розподілену мережу і HSM повинен бути захищеним від крадіжки та злому на фізичному рівні, що затрудняє використання даного модуля в розподілених системах. А також, сам інтерфейс для управління ключами через Інтернет є більш вразливим і відрізняється від тих, що використовуються локально, що

значно знижує рівень безпеки при використанні каналів зв'язку. *Вразливість генерації ключів.* Cloud Computing поєднує в собі технології віртуалізації та повністю виключає використання пристроїв ведення, що означає, що система має невеликий рівень ентропії. Тим самим, така віртуалізована система надає зловмиснику можливість підібрати ключі шифрування для віртуальних машин, використовуючи лише одну з віртуальних машин. Дана проблема призводить до серйозних наслідків, але також має декілька шляхів вирішення, тому повинна бути враховано обов'язково. *Вразливість обробки даних.* Шифрування даних не є складною задачею, але Cloud Computing не надає клієнтам можливість передачі ресурсів в зашифрованому вигляді, так як застосування алгоритму шифрування збільшує кількість процесорного часу. Отже, протягом довготривалого періоду часу клієнтам Cloud Computing залишається лише довіряти своїм провайдерам, тому що підтримання шифрування під час обробки даних практично не можлива. *Вразливість репутації.* Через використання Cloud Computing віртуальних машин, що залежать одна від одної, то діяльність одного клієнта впливає на репутацію іншого клієнта, що може призвести до побічних наслідків. *Вразливість ізоляції.* Використання ресурсів одним клієнтом може вплинути на ресурси, що використовується іншим клієнтом. В основі концепції «Інфраструктура як Сервіс» покладена архітектура, де фізичні ресурси є спільними для декількох віртуальних машин та мають декілька клієнтів. Вразливості в гіпервізорі можуть призвести до несанкціонованого доступу до розподілених ресурсів. *Вразливість інтерфейсу управління.* Гіпервізор, що використовується в концепції «Інфраструктура як Сервіс» парадигми Cloud Computing пропонує багатий API, що дає змогу провайдеру розробку власних засобів управління, підготовки та подання звітності та інших корисних інтерфейсів для своїх клієнтів. Вразливості в моделі безпеки гіпервізора або в «інтерфейсі управління» можуть призвести до несанкціонованого доступу до інформації про клієнта. У той же час вразливість на цьому рівні може дозволити зловмиснику маніпулювати активами об'єкта всередині Cloud Computing, викликаючи відмову в обслуговуванні (наприклад, виключення запущених віртуальних машин), витоку даних (наприклад, копіювання і передачу за межами Cloud Computing віртуальних машин), компрометування даних (наприклад, заміна віртуальної машини її модифікованою копією), або прямим фінансовим збиткам (наприклад, запуск багатьох копій віртуальних машин). *Вразливість моделювання ресурсів.* Система Cloud Computing є дуже вразливою для закінчення ресурсів, саме тому провайдери надають змогу клієнтам зарезервувати потрібні їм ресурси заздалегідь. При неспівпадіннях в процесі навантаження та забезпечення ресурсами алгоритм виділення ресурсів може мати хибне спрацьовування, що призведе до відсутності у клієнта необхідних ресурсів. *Вразливість зондування.* Так як Cloud Computing має внутрішню мережу, то кожен клієнт може виконати сканування портів та будь-які інші тести, що відносяться до роботи інших клієнтів в рамках внутрішньої мережі.

*Аутентифікація користувачів Cloud-сервісів***.** Концепція Cloud Computing є потужним інструментом для забезпечення нового рівня безпеки, використовуючи стандартні засобі захисту користувачів та персональних даних. Такі можливості Cloud-середовища, як стандартизація, автоматизація та поліпшений огляд інфраструктури здатні радикально підвищити рівень захищеності даних. Наприклад, використання заздалегідь заданого набору Cloud-інтерфейсів, поряд з централізованим управлінням ідентифікаційної інформацією та застосуванням політик управління доступом, зменшує ризик доступу користувачів до неналежних ресурсів. Необмежені обчислювальні ресурси дають змогу використовувати раніше недоступні алгоритмі шифрування, що забезпечують новий рівень захищеності персональних даних. Крім того, такі механізми, як автоматична ініціалізація і відновлення працюючих образів скорочують простір для потенціальних атак і дозволяють успішно вирішити ряд правових аспектів. Узгоджена політика управління правами і доступом потрібна для того, щоб гарантувати, що всі базові компоненти Cloud-сервісу підтримують конфіденційність даних і відповідають нормативним вимогам. Централізований сервіс управління правами дозволяє гарантувати формування та застосування єдиної політики для захисту конфіденційності клієнтів в масштабі всіх сервісів Cloud-середовища.

Постачальники Cloud-сервісів здатні підтримувати моделі SaaS і IaaS як всередині окремих Cloud-середовищ, так і з охопленням декількох Cloud-середовищ. Постачальник повинен орієнтуватися на оптимальні методики впровадження та забезпечувати клієнтам максимальний контроль над станом безпеки і нормативної відповідності Cloud-сервісів.

Можливості для спрощеного управління безпекою. Поява SAML (Security Assertion Markup Language) зробило можливим забезпечення безпеки програм Cloud Computing для сервіс провайдерів, які використовують протокол SOAP (Simple Object Access Protocol). SAML надає механізм, який дозволяє транспортувати параметри ідентифікації на всіх рівнях.

Сервіс STS (WS-Trust Security Token Service) дозволяє перетворювати параметри безпеки (token) з формату SAML в формат, специфічний для домену, і навпаки. Cloud Computing є шлюзом, який забезпечує сумісність різних програмних технологій. Останнім часом стала популярною технологія SOA (Service Oriented Architecture), яка часто поєднується з SOAP і REST (Representational State Transfer). Базовим принципом такої архітектури є забезпечення сумісності базових стандартів (XML, SOAP, WS-Security і HTTP). Коли джерело запиту Cloud Computing сервісу взаємодіє з сервіс провайдером, вони не повинні залежати від деталей, прихованих всередині конкретних програмних реалізацій. Взаємодія між ними відбувається за допомогою стандартних повідомлень. Більшість сервісів проводять аутентифікацію користувача системного або прикладного рівня. В результаті сервіс провайдер перевіряє ідентичність джерела запиту, аналізуючи, параметри ідентифікації. Ця модель не є цілком безпечною. В свою чергу сервіси Cloud Computing поліпшують безпеку використовуючи вбудовані механізми аутентифікації, наявні в транспортних протоколах, таких як HTTP і TLS. Таке рішення помітно покращує безпеку каналу. В результаті сервіс-провайдер може бути впевнений, що повідомлення надіслано вузлом, що заслуговують довіри. Однак вміст повідомлення залишається непідконтрольним і залишає можливість для атаки інсайдера.

Існує три відкриті стандарту - WSS (Web Services Security), SAML (Security Assertion Markup Language) і WS-Trust (Web Services Trust), які здатні гарантувати ідентифікацію користувача шляхом включення потрібної інформації в SOAP-запит.

Можливо використовувати наступні сервіси безпеки:

- Конфіденційність
- Цілісність
- Аутентифікація
- Авторизація

Однак, так як архітектура Cloud Computing передбачає можливість знаходження джерела запиту і сервера в різних доменах, суміщення аутентифікації і авторизації стає неможливим. WS-Security є стандартом безпеки, широко використовуваним практично у всіх SOAP-системах. WS-Security не визначає нового механізму безпеки, він описує, як використовувати існуючі стандарти безпеки для забезпечення конфіденційності, цілісності повідомлень, аутентифікації в рамках SOAP-повідомлень.

Аутентифікація і авторизація використовують різні профілі для передачі маркерів безпеки в заголовках повідомлень WS-Security. Такі маркери можуть містити ідентифікаційні дані користувача. Рішення про авторизації приймаються на підставі цієї інформації. Повторна аутентифікація для надання певного сервісу вже не потрібно - працює принцип SSO (Single Sign-On). WS-Security визначає профілі для різних типів маркерів безпеки. Сюди входять профілі для Kerberos, сертифікатів X.509, пар ім'я / пароль, тверджень SAML і ліцензій XRML. WS-Trust є стандартом OASIS (Organization for the Advancement of Structured Information Standards), який визначає протокол повідомлень для отримання чи перевірки маркерів безпеки, що генеруються службою STS (рис.1).

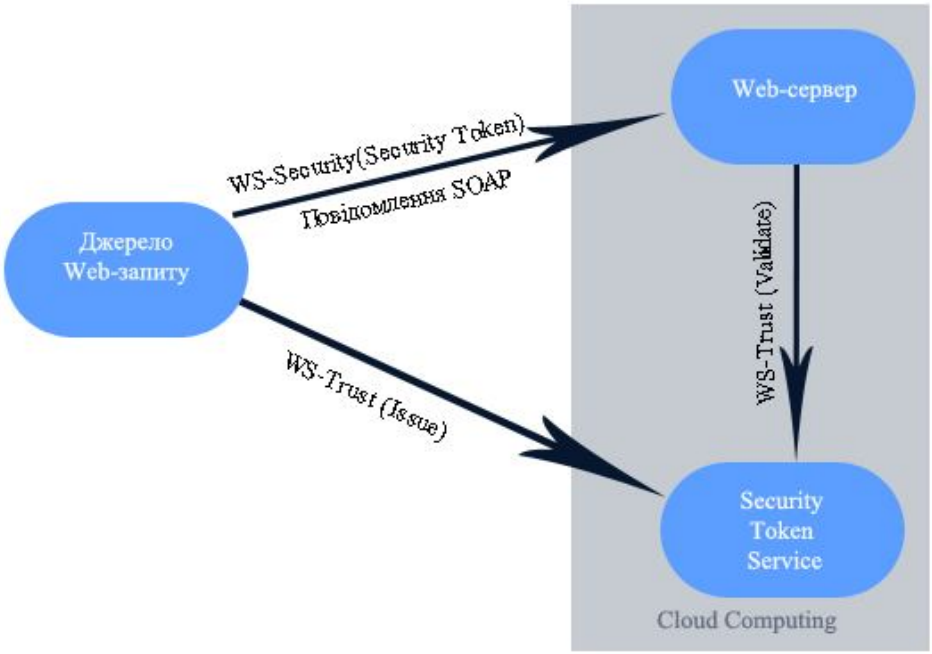

Рис.1. Безпека WS передає ідентифікаційні дані за допомогою Security Token, створеного STS

Обробка ансамблю ідентифікації є багатоступеневим і повторюваним процесом, який реалізується незалежно від протоколів і профілів, що використовуються для переміщення маркерів безпеки через мережу[3].

Процес обробки ансамблю ідентифікації включає в себе наступні три фундаментальні процедури:

- Аутентифікація і встановлення довіри. Аутентифікація необхідна, щоб перевірити ідентичність користувача (представлену маркером безпеки) в одному домені безпеки, перед генерацією іншого маркера безпеки, який забезпечить довіру до повідомлень в домені партнера. Довіра встановлюється в результаті обміну маркерами безпеки.
- Ідентичність користувача. Користувач може ідентифікуватися різними ідентифікаторами в різних доменах і в різних його ролях. Передбачається, що маркер безпеки містить у собі інформацію, що однозначно визначає особу і роль користувача. Ідентифікаційні дані можуть бути отримані з маркера або із зовнішніх інформаційних джерел, таких як LDAP-каталог.

Ідентифікаційна інформація може включати в себе значення атрибутів, таких як e-mail, роль, адреса, улюблений колір і т.д.

- Авторизація, аудит та надання даних. Аудит гарантує те, що відповідні дані користувача і його партнера залишаються коректними для SLA і відповідають існуючим вимогам. Інтегрована авторизація може бути базовою, гарантує, що в маркері безпеки є коректний ідентифікатор ролі користувача. Надання даних передбачає динамічне оновлення ідентифікаційних даних користувача, що зберігається в різних доменах (рис.2).

Висновки. Таким чином, детально проаналізувавши концепцію Cloud Computing можна зробити висновок, що дана концепція є досить цікавим інструментов для застосування в різних сферах IT-технологій. Особливо великий інтерес дана концепція має в сфері захисту інформації, оскільки можливості концепції Cloud Computing при достатньому рівні вивчення можуть запропонувати кардинально нові рішення для забезпечення безпеки.

Були проаналізовані аспекти безпеки використання Cloud Computing, розглянуті найбільш поширені ризики за вразливості, що пов'язані з Cloud Computing. Також проаналізована система аутентифікації, основні механізми аутентифікації, що використовує концепція Cloud Computing. Потрібно зазначити, що аутентифікація в концепції побудована на прикладі більшості Web-сервісів і використовує основні три стандарти: WSS (Web

Services Security), SAML (Security Assertion Markup Language) і WS-Trust (Web Services Trust).

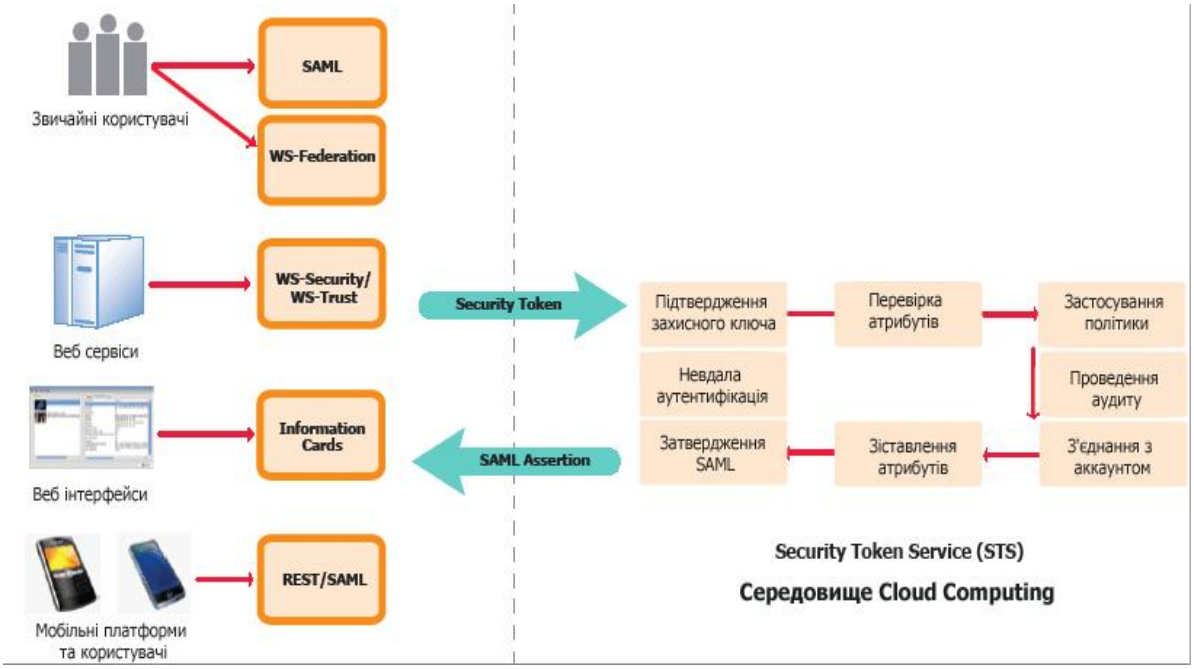

Рис.2. Сервіси маркерів безпеки транслюють їх затвердження в SAML

ЛІТЕРАТУРА

1. Hayes B. CloudComputing // Communications of the ACM.-2008.- P.9–11
2. McFedries P. The cloud is the computer // IEEE Spectrum Online.-2008
3. S. Lohr Google and I.B.M . Join in ‘Cloud Computing’

Надійшла: 15.12.2011

Рецензент: д.т.н., проф. Квасніков В.П.