© Partyka A., Zakharova Y. Security and data access control model in cloud services based on the identity and access management mechanism // Ukrainian Scientific Journal of Information Security, 2024, vol. 30, issue 1, pp. 12-20. ©

DOI: 10.18372/2225-5036.30.18575

МОДЕЛЬ БЕЗПЕКИ ТА КОНТРОЛЮ ДОСТУПУ ДО ДАНИХ У ХМАРНИХ СЕРВІСАХ НА ОСНОВІ МЕХАНІЗМУ IDENTITY AND ACCESS MANAGEMENT (IAM)

Андрій Партика, Ярина Захарова

Національний університет «Львівська політехніка»

ПАРТИКА Андрій Ігорович, к.т.н.
Рік та місце народження: 1984 рік, м. Львів, Україна.
Освіта: Національний університет «Львівська політехніка», 2006 рік.
Посада: старший викладач кафедри захисту інформації з 2015 року.
Наукові інтереси: безпека хмарних технологій та розподілених систем, методи і засоби захисту інформації в хмарах, бази даних та знань, безпека інфраструктури комп'ютерних мереж, етичний хакінг, AWS.
Публікації: більше 30 наукових публікацій, серед яких наукові статті, навчальний посібник, тези та матеріали доповідей на конференціях.
E-mail: andrijp14@gmail.com.
Orcid ID: 0000-0003-3037-8373.

ЗАХАРОВА Ярина Анатоліївна, студентка
Рік та місце народження: 2003 рік, м. Івано-Франківськ, Україна.
Освіта: повна загальна середня освіта.
Посада: студентка кафедри захисту інформації з 2020 року.
Наукові інтереси: кібербезпека, бази даних, шифрування, безпека хмарних технологій.
Публікації: 1 матеріали доповіді на конференції.
E-mail: yz.jobac@gmail.com.
Orcid ID: 0009-0006-0129-7944.

Анотація. *Впровадження хмарних сервісів дало можливість використовувати потужні ресурси та забезпечувати зберігання даних в безпечному місці з можливістю швидкого доступу. Проте, це стало значним джерелом небезпеки не тільки від зовнішніх зловмисників, а й від внутрішніх. Водночас стрімке збільшення використання хмарних сервісів в організаціях спричинило гостру необхідність в розроблені ефективної моделі безпеки та контролю доступу до даних, які зберігаються у хмарах, оскільки з'являються нові вразливості, які пов'язані з їхнім використанням. У роботі досліджується механізм Identity and Access Management, а також технології та стандарти, котрі широко використовуються для контролю доступу до даних чи моніторингу інцидентів інформаційної безпеки. Розробка моделі безпеки на основі IAM дозволяє встановлювати строгі правила доступу до даних, обмежувати привілеї користувачів та забезпечувати захист від несанкціонованого доступу. Також модель дозволяє ідентифікувати, автентифікувати та авторизувати користувачів, а також контролювати їх доступ до різних ресурсів і функцій хмарного сервісу, зменшуючи ризик інцидентів безпеки.*

Ключові слова: *модель безпеки, IAM, хмарні технології, автентифікація, авторизація, моніторинг, аудит, управління доступом.*

Постановка проблеми

Розвиток хмарних технологій змінив спосіб, яким організації зберігають, обробляють та надають доступ до своїх даних. Хмарні сервіси стали необхідним елементом інформаційної інфраструктури, забезпечуючи швидкий доступ до великого обсягу даних та високий рівень масштабованості. Однак, зростання використання хмарних сервісів викликає нові виклики щодо безпеки та контролю доступу до цих даних [1]. Однією з ключових проблем, з якими зіштовхуються організації, є забезпечення високого рівня безпеки та контролю доступу до даних у хмарних сервісах. Це стає особливо актуальним у контексті зростання кількості кібератак, витоків даних та регуляторних вимог щодо конфіденційності та цілісності інформації [2].

Для вирішення цих проблем розробка моделі безпеки та контролю доступу на основі механізму Identity and Access Management (IAM) виявляється надзвичайно важливою. IAM є стратегічним підходом до управління доступом до ресурсів хмарного сервісу та ідентифікації користувачів, що дозволяє контролювати та обмежувати їх права доступу до даних та функціональності [3].

Аналіз останніх досліджень і публікацій

Складність питання безпеки зростає в хмарній моделі, оскільки проблема тепер має додаткові виміри, такі як дані та конфіденційність, відсутність

навичок безпеки в хмарі та проблеми з захистом хмарних ресурсів. Доступ до даних у хмарі здійснюється онлайн і зберігається за допомогою сторонньої служби. У статті [4] автори досліджують проблему з точки зору моделей хмарних сервісів (SaaS, PaaS & IaaS). Такий підхід дозволяє отримати вичерпний опис проблеми з хмарною безпекою та ключовими функціями, які потрібно охопити.

У дослідженні [5] було створено модель, що допомагає вибирати з різноманітного спектру дій саме ті, які можна виконати для керування безпекою в хмарі. По суті це багатокритеріальну модель прийняття рішень на основі аналітичного ієрархічного процесу, яка може бути використана особами, які приймають стратегічні рішення, для вибору оптимального способу дії.

Щоб мінімізувати ризики, пов'язані з цими загрозами, пропонується модель, яка залежить від шифрування та стеганографії з метою застосування моделі безпеки в хмарному середовищі. Цей комплексний підхід ефективно захищає цілісність даних, конфіденційність і приватність від потенційних зловмисників. Крім того, він підвищує гнучкість і ефективність хмари, забезпечуючи безпечне зберігання та передачу великих обсягів даних [6, 7].

Мета і постановка завдання

Хмарна безпека поєднує політики, методи, підходи та технології до забезпечення кібербезпеки та захисту застосунків та даних у хмарних середовищах. Ключем до захисту від зовнішніх та внутрішніх загроз можуть стати детально опрацьовані політики управління доступом, дотримання галузевих та корпоративних вимог безпеки, використання інструментів для автоматизованого бекапування та аварійного відновлення даних [8]. Метою даного дослідження є розробка моделі безпеки та контролю доступу до даних у хмарних сервісах на основі механізму IAM. Дослідження буде зосереджено на вивченні принципів IAM, виявленні потенційних загроз. Така модель дозволить встановлювати строгі правила доступу до даних, обмежувати привілеї користувачів та забезпечувати захист від несанкціонованого доступу. Окрім того, вона може забезпечувати ідентифікацію, авторизацію та аутентифікацію користувачів, а також контролювати їх доступ до різних ресурсів і сервісів хмарного провайдера [9]. Важливою задачею також є розроблення рекомендацій для подальшого вдосконалення, оскільки створення та налаштування механізму чи моделі є першим базовим кроком, проте необхідно глибоко розуміти розроблену модель і заздалегідь будувати план оновлень [10].

Виклад основного матеріалу дослідження

Управління ідентифікацією та доступом (IAM) є структурою бізнес-процесів, політик і технологій, яка полегшує керування електронною або цифровою ідентифікацією. Завдяки системі IAM керівники інформаційних технологій (IT) можуть контролювати доступ користувачів до критично важливої інформації у своїх організаціях. Системи, які використовуються для IAM, включають системи єдиного входу, двофакторну автентифікацію, багатофакторну автентифікацію та керування привілейованим доступом. Ці технології також надають можливість безпечно зберігати ідентифікаційні дані та дані профілю, а також функції керування даними, щоб забезпечити спільний доступ лише до необхідних і актуальних даних [11].

Системи IAM можуть бути розгорнуті на місці, надані стороннім постачальником через хмарну модель підписки або розгорнуті в гібридній моделі.

Інфраструктура IAM дозволяє контролювати доступ користувачів до важливої інформації в їхніх організаціях. Продукти IAM пропонують контроль доступу на основі ролей, який дозволяє системним адміністраторам регулювати доступ до систем або мереж на основі ролей окремих користувачів на підприємстві. У цьому контексті доступ — це можливість окремого користувача виконувати певне завдання, наприклад переглядати, створювати або змінювати файл. Ролі визначаються відповідно до роботи, повноважень і відповідальності на підприємстві.

Системи IAM повинні робити наступне: отримувати та записувати інформацію про вхід користувача, керувати корпоративною базою даних ідентифікацій користувачів і організовувати призначення та видалення привілеїв доступу.

Це означає, що системи, які використовуються для IAM, повинні забезпечувати централізовану службу каталогів із наглядом і видимістю всіх аспектів бази користувачів компанії [12].

Технології IAM розроблені для спрощення процесу надання користувачам і налаштування облікового запису. Ці системи скорочують час, необхідний для завершення цих процесів, завдяки контрольованому робочому процесу, який зменшує кількість помилок і потенційні зловживання, одночасно дозволяючи автоматизувати виконання облікового запису. Система IAM також дозволяє адміністраторам миттєво переглядати та змінювати нові ролі та права доступу користувачів.

IAM включає компоненти та політики, необхідні для контролю та відстеження ідентифікаційних даних користувачів і привілеїв доступу до IT-ресурсів, середовищ і систем [13]. Зокрема, сервіси IAM існують як системи, що складаються з чотирьох основних компонентів керування:

- автентифікація: комбінації імені користувача та пароля залишаються найпоширенішими формами облікових даних користувача, якими керує система IAM, яка також може підтримувати цифрові підписи, цифрові сертифікати, біометричне обладнання (зчитувачі відбитків пальців), спеціалізоване програмне забезпечення (наприклад, програми аналізу голосу) і блокування;
- авторизація: компонент авторизації використовує служби атрибутів для визначення атрибутів і правил контролю доступу та контролює зв'язки між ідентифікаторами, правами контролю доступу та доступом до IT-ресурсів;
- керування користувачами: пов'язане з адміністративними можливостями системи, програма керування користувачами відповідає за створення нових облікових записів користувачів і груп доступу, скидання паролів, визначення політики паролів і керування привілеями;
- керування обліковими даними: система керування обліковими даними встановлює ідентифікаційні дані та керує ними шляхом видачі облікових даних.

Основні концепції системи включають автентифікацію споживачів і визначення авторизації шляхом посилання на атрибути споживача, атрибути ресурсу та середовище. Для цього потрібно керувати даними IAM, включаючи керування обліковими даними споживача та керування атрибутами. Реплікація даних IAM між хмарою та локальними базами даних, що підтримує рішення щодо контролю доступу, а також керування користувачами та обліковими даними (рис. 1). Механізми автентифікації та авторизації мають бути розташовані в мережі, для якої вони використовуються [14].

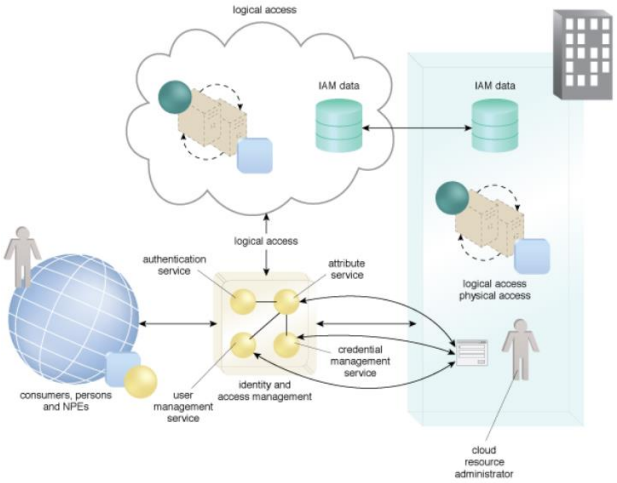

Рис. 1. Приклад операційної концепції IAM

Identity and Access Management (IAM) пропонує кілька архітектурних шаблонів, які можна використовувати для проектування рішень управління доступом. Кожна з архітектур має свої переваги та недоліки, які варто враховувати при виборі підходящого рішення для конкретної організації.

Централізована архітектура IAM забезпечує централізоване керування доступом та політиками, забезпечуючи послідовність та однорідність. Однак, ця архітектура може стати окремим центром залежності та створити ризики, якщо виникнуть проблеми з центральною системою.

Децентралізована архітектура IAM надає більшу автономію та гнучкість для окремих підрозділів або сервісів в організації. Кожен підрозділ може мати власний набір політик та прав доступу, що спрощує управління на рівні локальних потреб. Проте, можуть виникнути складнощі з координацією та забезпеченням однорідності між різними системами.

Архітектура федерації IAM дозволяє обмінюватись ідентифікаційною та авторизаційною інформацією між різними організаціями або довіреними сторонами. Це дозволяє розширити контроль доступу та спільно використовувати ідентифікаційні дані без повторної автентифікації. Однак, необхідно враховувати ризики пов'язані зі зовнішніми системами та забезпеченням безпеки в обміні інформацією.

Архітектура міжхмарного доступу IAM забезпечує масштабованість та гнучкість для великих компаній, де потрібно керувати доступом до різних ресурсів. Вона дозволяє налаштовувати права доступу відповідно до потреб організації, проте може потребувати складнішої настройки та управління.

Архітектура з дрібним контролем доступу IAM дозволяє встановлювати деталізовані права доступу для кожного користувача або групи користувачів. Це дозволяє точно налаштувати доступ до різних ресурсів, проте може вимагати більшої уваги до управління та підтримки системи.

Архітектура IAM для мікросервісів забезпечує управління доступом до мікросервісів у розподіленому середовищі. Ця архітектура спрощує управління доступом до окремих сервісів, проте може потребувати додаткових механізмів для забезпечення безпеки та захисту даних між сервісами.

Як бачимо, кожна архітектура IAM має свої переваги та недоліки, які необхідно враховувати при виборі підходящого рішення для конкретної організації. Враховуючи особливості своєї бізнес-моделі, організації повинні здійснити аналіз та оцінку архітектур, щоб забезпечити ефективне управління ідентифікацією та доступом до ресурсів [15].

Управління ідентифікацією та доступом (IAM) передбачає відстеження поведінки та дій кожної особи та активу в IT-середовищі, зокрема ваших системних адміністраторів і критично важливих активів. Це особливо складно через постійну природу та широкі характеристики підключення наших взаємопов'язаних систем.

Структура пропонованої моделі базується на шести основних критеріях: операційна досконаліть, безпека, надійність, ефективність та продуктивність, оптимізація витрат та стійкість.

При розробці дотримувались принципи:

1. Запровадження надійної ідентифікації. Реалізовується принцип найменших привілеїв і розподіляються обов'язки з відповідним дозволом для кожної взаємодії з ресурсами. Керування ідентифікацією відбувається централізовано;
2. Підтримування постійного моніторингу. Відстежування, моніторинг, сповіщення та перевірка дій чи/та змін у середовищі в режимі реального часу;
3. Автоматизація методів безпеки;
4. Захист даних під час передавання та зберігання. Класифікація даних за рівнями конфіденційності та використання шифрування або токенізації чи контролю доступу;
5. Утримання людей подалі від даних. Використання інструментів для зменшення чи усунення потреби в прямому доступі або в ручній обробці даних. Це зменшило ризик неправильної обробки чи модифікації даних;
6. Підготовка до подій та інцидентів безпеки.

Також варто зазначити, що керування ідентифікаційним доступом може використовувати кілька технологій, щоб контролювати, хто може переглядати дані. Ці елементи керування включають: багатофакторна аутентифікація, єдиний вхід, керування паролями та керування профілем. Розробляючи систему, бралось до уваги, що управління ідентифікацією стосується п'яти політик, які повинні бути включені в основу, щоб модель була успішною:

1. Як система ідентифікує співробітників та клієнтів;
2. Як визначаються ролі та розподіляються між працівниками;

3. Як система повинна дозволяти додавати, вилучати та оновлювати співробітників і їхні ролі;

4. Дозвіл призначення групам або окремим особам відповідних рівнів доступу;

5. Захист конфіденційних даних та захист системи від злому.

Ці п'ять політик нададуть працівникам доступ до необхідних даних, водночас гарантуючи, що компанії дотримуються всіх законів про конфіденційність [16].

Архітектури управління ідентифікацією та доступом (IAM) забезпечують інфраструктуру для захисту даних і ресурсів [17]. Внутрішні мережі встановлюють кордони безпеки в локальних системах. У хмарних середовищах мереж периметра та брандмауерів недостатньо для керування доступом до програм і даних. Натомість публічні хмарні системи покладаються на рішення ідентифікації для безпеки кордонів [18]. Нижче наведені основні елементи архітектури розробленої моделі:

1. Увімкнення незмінних приватних ідентифікаторів чи змінних публічних. У будь-якій системі IAM користувач ідентифікується за допомогою одного або кількох ідентифікаторів. Вони можуть включати ім'я користувача, адресу електронної пошти, номер телефону, номер страхового поліса або будь-який ідентифікатор, унікальний для системи. Користувач має можливість вибрати будь-який із них, щоб підтвердити себе та отримати доступ до системи. Ці публічні ідентифікатори є змінними. Користувач повинен мати можливість змінити їх без жодного впливу на систему. Це створює необхідність мати приватний ідентифікатор, який є незмінним. Приватний ідентифікатор – це ідентифікатор, згенерований системою, який є унікальним у всій системі, ніколи не передається користувачеві та є лише внутрішнім для системи. Необхідно мати єдине місце в системі, яке зіставляє цей приватний ідентифікатор з одним або декількома загальнодоступними ідентифікаторами певного користувача. Окрім цієї таблиці зіставлення, публічні ідентифікатори користувачів ніколи не використовуються в системі для будь-яких посилань, використовується лише приватний ідентифікатор. Під час події входу наданий загальнодоступний ідентифікатор зіставляється з відповідним приватним ідентифікатором, який використовується для автентифікації користувача. Усі журнали аудиту та аналітика зберігаються за приватним ідентифікатором. Оскільки підтримуємо всі внутрішні посилання певного користувача за допомогою незмінного ідентифікатора, зміни загальнодоступних ідентифікаторів не матимуть жодного впливу на систему;

2. Відокремлення основної/статичної інформації, яка дозволяє ідентифікувати особу(PII), від Transactional Data. Відповідно до NIST (National Institute of Standards and Technology), персональна інформація (PII) відноситься до будь-якої інформації про особу, яку зберігає організація, включно з будь-якою інформацією, яка може бути використана для розрізнення або відстеження особистості клієнта (така як ім'я, номер соціального страхування, дата та місце народження, дівоче прізвище матері або біометричні записи) або будь-яку іншу інформацію, яка пов'язана або може бути пов'язана з особою (наприклад, медична, освітня, фінансова чи інформація про роботу). Статичні (або близькі до статичних) ідентифікаційні дані – це ваше ім'я, прізвище, електронна адреса, номер телефону, номер соціального страхування тощо. Інші дані, які можна зв'язати з користувачем – це медичні записи, освітні/фінансові записи, шаблони входу тощо. Під час створення інфраструктури IAM дані транзакцій мають бути відокремлені від статичних ідентифікаційних даних, і їх можна зв'язати за допомогою автоматично створеного, незмінного ідентифікатора системи, який згадувався вище. Це розділення допомагає масштабувати дані транзакцій незалежно від статичних ідентифікаційних даних. Крім того, це розділення вирішує проблеми конфіденційності даних, оскільки не потрібно турбуватися про шифрування будь-яких транзакційних даних, крім ідентифікаційних даних і таблиці зіставлення (яка зіставляє ідентифікаційні дані з автоматично створеним незмінним системним ідентифікатором).

3. Відокремлення біометричних даних від інших ідентифікаційних даних. Біометрична реєстрація та зіставлення виконується спеціальним біометричним механізмом, який зберігає біометричні шаблони для користувача. Тут повинні відокремити ідентифікаційну інформацію від біометричних даних, і найпростіший спосіб зробити це — отримати хеш незмінного приватного ідентифікатора (який є псевдонімом) і зберегти його разом із біометричними даними. Той, хто збирає біометричні дані, не зможе пов'язати їх із ідентифікаційною інформацією відповідного користувача. Навіть якщо зловмисник отримає доступ і до ідентифікаційної інформації, і до сховищ біометричних даних, йому/їй все одно доведеться переглянути всі незмінні приватні ідентифікатори, хешувати їх і потім знайти збіг. Однак слід пам'ятати, що відбувається шифрування приватного ідентифікатору у таблиці відповідності ідентифікаційної інформації, тому зловмиснику також необхідно отримати доступ до відповідних ключів, що набагато більше ускладнює роботу зловмисника;

4. Запровадження зовнішніх правил контролю доступу. Правила контролю доступу є відображенням вимог бізнесу. Вони повинні бути представлені таким чином, щоб зміни в бізнес-вимогах могли бути включені в правила контролю доступу з мінімальним впливом чи зусиллями. Необхідно побудувати архітектуру для адміністрування політики, її застосування, оцінки політики та зберігання політики. При створенні з нуля, рекомендовано використовувати XACML (eXtensible Access Control Markup Language), адже він представляє еталонну архітектуру, мову політики та протокол запиту/відповіді. Еталонна архітектура XACML визначає точку адміністрування політики (PAP), точку прийняття рішень (PAP), точку застосування політики (PEP), точку інформації про політику (PIP) і взаємодію між ними. Мова політики в XACML базується на XML. Він досить багатий з точки зору можливостей, але він не зовсім простий і вимагає певних зусиль щодо підтримки інструментів. Модель запиту/відповіді XACML може базуватися на XML або JSON, а взаємодію між PEP і PDP можна стандартизувати за допомогою REST API. Варто зауважити, що спочатку потрібно подбати про вимоги до

контролю доступу, а потім вирішити, як представити їх як політики;

5. Переконатись, що сутності з низьким рівнем довіри не мають доступу на запис. Кожен компонент у мережі має рівень довіри. Ключові компоненти розгортання IAM включають постачальник ідентифікаційних даних (IdP), сховище ідентифікаційних даних (ldap / база даних), сховище метаданих/політики, шлюз (точка застосування політики) і, нарешті, постачальники послуг. Кожен із цих компонентів або деякі з них можуть перебувати в різних рівнях довіри. Створення та проектування інфраструктури IAM на різних рівнях довіри допомагає децентралізувати відповідальність і право власності на основі рівня довіри;

6. Відокремлення B2C (Business-to-consumer) від B2E (business to employee) і B2B (business-to-business). У B2E IAM за адаптацію відповідає роботодавець, тоді як у B2C це здебільшого самостійна адаптація. B2E/B2B IAM також відомий як робоча сила (workforce) IAM. Робоча сила IAM дивиться всередину, зосереджується на взаємодії B2E (бізнес-співробітник) і B2B (бізнес-бізнес). Метою IAM для робочої сили є зменшення ризиків і витрат, пов'язаних із залученням і відключенням нових співробітників, партнерів і постачальників, тоді як метою IAM для клієнтів (або B2C) є сприяння збільшенню доходів шляхом використання ідентифікаційних даних для отримання та утримання клієнтів. Основне завдання IAM для робочої сили полягає в тому, щоб зруйнувати розрив ідентифікації на підприємстві та створити єдину платформу ідентифікації, яка призведе до підвищення продуктивності, безпеки, управління, нагляду, відповідності та моніторингу. Зрештою, це зменшить як ризик, так і витрати, пов'язані з усіма взаємодіями B2E та B2B;

7. Забезпечення постійних псевдонімів для спільного використання атрибутів. Всі інші компоненти в корпоративній мережі (і за її межами) довіряють твердженням, виданим постачальником ідентифікаційної інформації. Ці твердження можуть бути твердженнями автентифікації, твердженнями атрибутів або твердженнями авторизації. Твердження прив'язані до автентифікованого суб'єкта. Рекомендований підхід полягає в тому, щоб користувач або постачальник послуг використовували постійний псевдонім. Кожен користувач матиме інший псевдонім для кожного постачальника послуг і зіставляється з його приватним незмінним ідентифікатором у постачальника ідентифікаційної інформації. Кожен постачальник послуг може використовувати цей псевдонім як дескриптор кореляції;

8. Дотримання загальноприйнятих стандартів. Важливо зазначити, що сьогодні жоден ідентифікаційний продукт не зможе отримати жодних конкурентних переваг, лише підтримуючи відкриті стандарти ідентифікаційної інформації, оскільки це є даним і очікуваним для будь-якого продукту ідентифікаційної інформації. Тим не менш, якщо створюється ідентифікаційний продукт, який не підтримує відкриті стандарти, він фактично є неконкурентоспроможним;

9. Увімкнення Self-Expressive облікових даних. Захист облікових даних користувача є ключовим аспектом будь-якої інфраструктури IAM. Ці облікові дані можуть бути просто паролями або будь-якими ключами. Існує два типи облікових даних, які зберігаються в інфраструктурі IAM. Ті, якими ви володієте (або випускаєте), і ті, якими ви користуєтеся. Перший тип облікових даних може бути захищений за допомогою хешу, а другий тип має бути захищений шифруванням. Тобто, коли хешуються облікові дані, необхідно обов'язково прив'язати алгоритм хешування до самих хешованих облікових даних. При перевірці облікових даних, самі облікові дані будуть самовиразними. Якщо зробити облікові дані самовиразними, ви знаєте, як перевірити кожне з них незалежно. Більше того, за допомогою цього підходу, якщо знайдете будь-які облікові дані, які зберігаються за алгоритмом хешування, який відрізняється від параметрів системи, можете повторити хешування з новим і оновити систему на момент перевірки;

10. Розглядання привілейованих облікових записів як окремий вид. В інфраструктурі IAM існує кілька випадків, коли використовуються привілейовані облікові записи. Облікові дані бази даних, облікові дані сховища ідентифікаційних даних (активний каталог), облікові дані адміністратора IAM (можливо, доступ до веб-консолі керування для виконання функцій адміністратора IAM), а також облікові записи інших сторонніх систем/служб (доступ до API IAM для виконання адміністративних функцій) усі підпадають під категорію привілейованих облікових записів. Керування привілейованими ідентифікаційними даними (PIM) є ключовою сферою IAM, і існують спеціалізовані постачальники, які розробляють продукти, які підтримують PIM. Створюючи будь-яку серйозну інфраструктуру IAM, потрібно турбуватися про те, як система інтегрується з продуктами PIM. Крім того, необхідно мати систему PIM, щоб відповідати галузевим вимогам, таким як SOX, PCI-DSS, HIPAA, FISMA, BASEL III та багатьом іншим.

Основні компоненти моделі [19]:

1. Ідентифікація та аутентифікація:

- використання централізованої системи ідентифікації та аутентифікації для всіх користувачів і сервісів;
- використання сильних методів аутентифікації, таких як багатофакторна аутентифікація, для підвищення рівня безпеки;

2. Управління доступом:

- використання політик управління доступом для керування правами користувачів і ролей;
- встановлення принципу найменших привілеїв, щоб обмежити доступ до ресурсів тільки необхідним користувачам;
- використання ролей для групування прав доступу та спрощення управління;

3. Аудит та моніторинг:

- запис та аналіз подій доступу до ресурсів для виявлення можливих загроз безпеці та недоліків в системі;
- використання механізмів моніторингу для виявлення незвичайної активності та потенційних атак;

4. Шифрування даних:

- використання шифрування для захисту конфіденційності даних під час транзиту та зберігання;

- використання ключів шифрування з обмеженими правами доступу для забезпечення контролю над доступом до зашифрованих даних;

5. Захист мережі: використання механізмів захисту мережі, таких як брандмауери, для обмеження доступу до хмарних ресурсів тільки з довірених мереж.

Користувачі інфраструктури зазвичай є адміністраторами, операторами та розробниками. Користувачі не використовують портал клієнтів і не потребують контролю доступу. Нижче наведено області, на яких можна базувати дозволи користувача (табл. 1).

Таблиця 1

Рекомендації дозволів

Сфера	Дозвіл
Адміністрування	Надання користувачам-адміністраторам дозвіл додавати користувачів, переглядати дії облікових записів, редагувати профіль компанії, скидати паролі, оновлювати платіжні дані, надсилати одноразові платежі та керування сервером. Важливо залишити можливість встановлювати або скасовувати ці дозволи одним клацанням миші або надавати користувачеві окремий дозвіл для кожної дії.
Підтримка	Дозвіл у зоні підтримки дає користувачеві можливість перезапускати віртуальні машини (VM) і виконувати всі дії, пов'язані з заявками на підтримку, включаючи перегляд, оновлення та створення заявок.
Безпека	Дозволи в області безпеки дозволяють користувачеві керувати декількома важливими для безпеки областями, такими як SSL або SSH сертифікат і керування ключами, доступ до брандмауерів і сканування вразливостей.
Обладнання	Дозволи на апаратне забезпечення дають користувачеві доступ до перегляду деталей обладнання, перезапуску або керування системою, керування моніторингом сервера, перезавантаження операційної системи, редагування імен хостів і доменів.
Програмне забезпечення	У цій області користувач отримує дозвіл на перегляд кількох програмних продуктів.
Приватна мережа	У цій області можете надати мережеві дозволи низького рівня, пов'язані з VLAN, тунелями, керуванням портами тощо.

Додатково до описаних компонентів моделі безпеки та контролю доступу на основі механізму IAM, розглянемо деякі інструменти, технології та механізми, які можна використати для її реалізації:

- рівні доступу – використання рівнів доступу для класифікації ресурсів та обмеження доступу в залежності від їх конфіденційності та важливості;
- ролеве управління доступом – використання систем управління ролями (Role-Based Access Control, RBAC) для надання доступу до ресурсів на основі ролей, що спрощує управління правами користувачів;
- централізовані системи IAM – використання розширених централізованих систем IAM, таких як Okta, Azure Active Directory, OneLogin тощо, для керування ідентифікацією, аутентифікацією та авторизацією користувачів;
- федерація та одноразові токени: використання протоколів федерації, таких як SAML (Security Assertion Markup Language) або OpenID Connect, для безпечного обміну ідентифікаційною інформацією між різними організаціями або сервісами. Використання одноразових токенів (nonce) для забезпечення безпеки та унікальності ідентифікаційних запитів;
- шифрування та ключові системи: використання симетричного або асиметричного шифрування для захисту конфіденційності даних. Використання систем управління ключами (Key Management Systems, KMS) для генерації, зберігання та управління ключами шифрування;
- механізми аудиту та моніторингу: використання системи централізованого аудиту та моніторингу подій доступу для виявлення ненормальної активності, несанкціонованого доступу та вразливостей системи;
- двофакторна аутентифікація: використання додаткових методів аутентифікації, таких як одноразові паролі, апаратні ключі або біометричні дані, для забезпечення більш високого рівня безпеки при вході в систему.

Ці інструменти, технології та механізми можуть бути використані для розширення та покращення моделі безпеки та контролю доступу на основі механізму IAM у хмарних сервісах. Вибір конкретних засобів залежить від потреб організації, рівня безпеки, типу даних та характеристик самого сервісу.

До переваг розробленої моделі можна віднести:

- забезпечення централізованого та ефективного управління доступом до хмарних ресурсів;
- зниження ризику несанкціонованого доступу та витоку даних шляхом точного контролю доступу до ресурсів;
- покращення безпеки даних шляхом використання сильних методів аутентифікації та шифрування;
- забезпечення послідовності та однорідності в управлінні доступом до різних хмарних сервісів.

Однак варто відзначити також і певні особливості моделі, які можна трактувати в певних випадках як недоліки:

- потребує додаткових зусиль та ресурсів для реалізації та підтримки централізованої системи управління доступом;
- можлива складність налаштування та управління правами доступу, особливо в великих організаціях зі складною ієрархією користувачів та ролей.

Ця модель безпеки та контролю доступу на основі механізму IAM є потужним інструментом для забезпечення безпеки та конфіденційності даних у хмарних сервісах. Вона дозволяє організаціям ефективно управляти доступом до ресурсів, знижувати ризики

безпеки та забезпечувати довіру в інфраструктуру хмарних сервісів. Однак, при впровадженні цієї моделі необхідно ретельно розглянути вимоги та особливості організації, а також забезпечити належне навчання та свідоме використання механізму IAM для оптимального захисту даних [20].

Рекомендації щодо майбутнього покращення запропонованої моделі безпеки:

- впровадження моніторингу та інцидент-менеджменту – запроваджуйте систему моніторингу, яка буде виявляти аномалії, підозрілу активність та вразливості. Встановіть процес інцидент-менеджменту, щоб швидко реагувати на потенційні загрози та вживати заходів для вирішення проблем;
- використання машинного навчання та штучного інтелекту – використання машинного навчання та штучного інтелекту може допомогти виявляти та прогнозувати загрози, автоматизувати процеси виявлення вразливостей та забезпечити більш точний аналіз безпеки [21];
- використання розширених сценаріїв доступу – можливість розширення сценаріїв доступу, таких як управління доступом на основі контексту, динамічне призначення ролей або використання атрибутів користувачів для точного контролю доступу. Це дозволить забезпечити більш гнучкий та пристосований підхід до управління доступом;
- проведення тренінгів з безпеку серед співробітників – проводьте регулярні навчання та освіту з питань безпеки серед співробітників, наголошуючи на найновіших загрозах та техніках атак. Співробітники повинні бути свідомі ризиків та дотримуватися кращих практик безпеки;
- шифрування на різних рівнях – впроваджуйте можливість використання шифрування на різних рівнях, включаючи шифрування даних у спокої, під час передачі та в споживачі. Це забезпечить додатковий захист конфіденційності даних [22];
- проведення аудиту безпеки – регулярно проводьте аудит безпеки для перевірки ефективності вашої моделі безпеки та виявлення можливих слабких місць. Аудит допоможе виявити пропуски та недоліки, що потребують уваги та вдосконалення [23];
- співпраця з постачальниками хмарних сервісів – встановіть ефективний механізм співпраці з постачальниками хмарних сервісів щодо безпеки та контролю доступу. Перевіряйте їхні практики безпеки, сертифікації та регулярно оцінюйте ризики, пов'язані з використанням їхніх сервісів [24];
- розроблення бізнес-плану для безпеки – створіть докладний бізнес-план, який охоплює всі аспекти безпеки та контролю доступу. Визначте цілі, стратегії та дії, необхідні для забезпечення безпеки в хмарних сервісах на основі моделі IAM;
- постійне вдосконалення моделі – технології та загрози безпеки постійно змінюються, тому важливо постійно вдосконалювати свою модель безпеки. Вивчайте нові методи та інструменти, впроваджуйте кращі практики і залучайте експертів для оцінки та рекомендацій;
- реагування на інциденти та навчання моделі – якщо сталася безпекова подія, реагуйте швидко, дізнавайтеся причину і вживайте заходів для запобігання їх повторенню. Приділяйте увагу вивченню вразливостей та вдосконаленню процесів безпеки на основі отриманих знань [25];
- залучення команди експертів з безпеки – важливо мати команду експертів з безпеки, яка буде відповідальна за розробку, впровадження та підтримку моделі безпеки. Експерти зможуть виявити потенційні загрози та надати рекомендації з покращення безпеки.

Висновки. У роботі було розглянуто та наведено основні загрози для хмарних сервісів, а саме: неправильна конфігурація сервісу, несанкціонований доступ, використання незахищених інтерфейсів, викрадення акаунтів, відсутність видимості та зовнішній обмін даними. До кожної загрози наведено варіанти вирішення та уникнення проблеми.

У роботі також було описано сервіс IAM та його значну роль у забезпеченні безпеки даних у хмарних сервісах. Визначено, що це структура бізнес-процесів, політик і технологій, яка полегшує керування електронною або цифровою ідентифікацією. Були розглянуті та наведені компоненти сервісу IAM, технології та стандарти, які використовуються для контролю доступу до даних у хмарних сервісах. Підкреслено необхідність використання ролей та токенів у сервісі IAM. Для порівняння та конструктивної оцінки наведені переваги та недоліки сервісу.

Завдяки системі IAM керівники інформаційних технологій (IT) можуть контролювати доступ користувачів до критично важливої інформації у своїх організаціях. Технології, які використовуються, також надають можливість безпечно зберігати ідентифікаційні дані та дані профілю, а також функції керування даними, щоб забезпечити спільний доступ лише до необхідних і актуальних даних.

При порівнянні основних шаблонів моделі безпеки було визначено їх недоліки та переваги, що допомогло створити систему, яка враховує більшість недоліків та має значні переваги.

Було розроблено та описано модель безпеки, в основу, якої лягли принципи надійної ідентифікації, підтримування постійного моніторингу, автоматизація методів, захист даних та підготовка до подій та інцидентів безпеки. Крім того, модель IAM може підтримувати багатофакторну аутентифікацію та інші механізми безпеки, що підвищують рівень захисту даних в хмарних сервісах. Це допомагає запобігти несанкціонованому доступу та збільшує загальну безпеку організації.

Однак, ефективність розробленої моделі IAM може залежати від правильного налаштування, управління та відповідності до безпекових стандартів та регуляторних вимог. Необхідно також враховувати фактори, які можуть вплинути на продуктивність, наприклад, обсяг даних, кількість користувачів та ресурсів. Загальною оцінкою ефективності моделі безпеки та контролю доступу до даних в хмарних сервісах на основі IAM буде реальне тестування та аудит розробленої моделі, а також врахування специфічних потреб та контексту організації.

Список літератури

[1]. Rayapati, Siri & Muttavarapu, Sravya & Nagasuri, Navya & Singhal, Sunita. (2023). Security in Cloud

Technologies: A Brief Overview. pp. 683-695. 10.4028/p-4pq758.

[2]. Kizza, Joseph. (2024). Cloud Computing Technology and Security. 10.1007/978-3-031-47549-8_23.

[3]. "Identity Access Management (IAM) System", TechTarget [Електронний ресурс]: https://www.techtarget.com/searchsecurity/definition/identity-access-management-IAM-system.

[4]. Kumar, Akhil & Vesireddy, Akhil Kumar Reddy & Shetty, Sharan. (2023). Cloud computing security issues in delivery service models and solutions. 10.13140/RG.2.2.23286.98882.

[5]. Rizvi, Zainab & Khan, Chaudry & O'Sullivan, Michael. (2023). Analytical hierarchy process model for managing cloud security. Information & Computer Security. 32. 10.1108/ICS-07-2022-0121.

[6]. Awadh, Wed & Alasady, Ali & Hashim, Mohammed. (2023). A multilayer model to enhance data security in cloud computing. Indonesian Journal of Electrical Engineering and Computer Science. 32. pp. 1105-1114. 1105. 10.11591/ijeecs.v32.i2.

[7]. Malleswari, B. & Kolachalama, Rakshita & Srivallii, Voruganty. (2023). Performance Evaluation of ML-Based AWS Security Evaluation Model for Cloud Computing. 10.1007/978-981-99-1588-0_59.

[8]. Vakhula, O., Opirskyy, I., Mykhaylova, O. Research on Security Challenges in Cloud Environments and Solutions based on the security-as-Code Approach, Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3550, (2023), pp. 55-69.

[9]. Shevchuk, D., Harasymchuk, O., Partyka, A., Korshun N. Designing Secured Services for Authentication, Authorization, and Accounting of Users, Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3550, (2023), pp. 217-225.

[10]. Solanki, Madan & Tokekar, Vrinda. (2022). Design and Implementation of Strong Security Architecture for Amazon Web Service based on Cloud Applications. International Journal of Innovative Technology and Exploring Engineering. 11. 17-22. 10.35940/ijitee.L9324.111-11222.

[11]. Identity Access Management (IAM) System, TechTarget [Електронний ресурс]: https://www.techtarget.com / searchsecurity / definition / identity-access-management-IAM-system.

[12]. Identity and Access Management, Cloud Computing Patterns [Електронний ресурс]: https://patterns.arcitura.com/cloud-computing-patterns/mechanisms/identity_and_access_management.

[13]. Elisa Bertino; Kenji Takahashi, Identity Management: Concepts, Technologies, and Systems, Artech, 2010.

[14]. "Integrated Identity and Access Management Architectural Patterns", Huihoo Open Source Community [Електронний ресурс]: https://book.huihoo.com/ibm-redbooks/security/redp4423-integrated-identity-and-access-management-architectural-patterns.pdf.

[15]. Integrated Identity and Access Management Architectural Patterns, IBM Redbooks [Електронний ресурс]: https: //www.ibm.com / downloads / cas /9Y-BEK41O.

[16]. Top Cloud Security Issues, Threats, and Concerns, Check Point Software Technologies Ltd. [Електронний ресурс]: https: // www.checkpoint.com / cyber-hub/cloud-security/what-is-cloud-security/top-cloud-security-issues-threats-and-concerns/.

[17]. Dubey, Parul & Tiwari, Arvind & Raja, Rohit. (2023). Introduction To Cloud Computing and AWS. 10.2174/978981516582112301000 2.

[18]. Gandhi, Raj & Shahji, Vivek & Kamble, Nitin. (2021). Access Control Model Based on AWS IAM. International Journal of Innovative Research in Computer and Communication Engineering. 9. 14508. 10.15680 / IJIRCCE.2021.0911024.

[19]. How to Build an Identity and Access Management Architecture, RSI Security [Електронний ресурс]: https://blog.rsisecurity.com/how-to-build-an-identity-and-access-management-architecture/.

[20]. Identity and Access Management Benefits, Identity Management Institute [Електронний ресурс]: https://identitymanagementinstitute.org/identity-and-access-management-benefits/.

[21]. Malleswari, B. & Kolachalama, Rakshita & Srivallii, Voruganty. (2023). Performance Evaluation of ML-Based AWS Security Evaluation Model for Cloud Computing. 10.1007/978-981-99-1588-0_59.

[22]. Ramadevi, J. & Dhar, M. & Kasiviswanadham, Y. & Majji, Sankararao & Kapila, Dhiraj. (2023). Cloud Infrastructure Security Using a Hybrid AES Encryption Model. 10.1007/978-981-99-1726-6_24.

[23]. Carrera, Gary. (2021). BUILDING A COMPREHENSIVE CLOUD SECURITY AUDIT PROGRAM. EDPACS. 66. 1-4. 10.1080/07366981.2021.2004689.

[24]. Dubey, Parul & Tiwari, Arvind & Raja, Rohit. (2023). Identity and Access Management in AWS. 10.2174/978981516582112301000 3.

[25]. Munteanu, Victor & Edmonds, Andy & Bohnert, Thomas & Fortiş, Teodor-Florin. (2015). Cloud Incident Management, Challenges, Research Directions, and Architectural Approach. Proceedings, 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing, UCC 2014. 786-791. 10.1109/UCC.2014.128.

УДК 004.056.5

Partyka A., Zakharova Y. Security and data access control model in cloud services based on the identity and access management mechanism

Abstract. *Implementation of cloud services has provided the opportunity to utilize powerful resources and ensure data storage in a secure location with fast accessibility. However, it has become a significant source of risk not only from external attackers but also from internal threats. At the same time, the rapid increase in the use of cloud services in organizations has caused an urgent need to develop an effective security model and control access to data stored in the clouds, as new vulnerabilities associated with their use appear. The research focuses on investigating the IAM mechanism, as well as technologies and standards widely used for data access control and monitoring of information security incidents. A security and access control model has been developed, as well as recommendations for improving the*

system. Developing a security model based on IAM allows you to set strict data access rules, limit user privileges, and provide protection against unauthorized access. Also, the model allows users to be identified, authenticated and authorized, as well as control their access to various resources and functions of the cloud service, reducing the risk of security incidents.

Keywords: *security model, IAM, cloud technologies, authentication, authorization, monitoring, auditing, access management.*

Партика Андрій Ігорович, к.т.н., старший викладач кафедри захисту інформації Національного університету «Львівська політехніка».

Andrii Partyka, Ph.D., Senior Lecturer the Department of Information Security, Lviv Polytechnic National University.

Захарова Ярина Анатоліївна, студентка, спеціальності 125 Кібербезпека Національного університету «Львівська політехніка».

Yaryna Zakharova, student the Department of Information Security, Lviv Polytechnic National University.

Отримано *19 січня 2024 року*, затверджено редколегією *1 квітня 2024 року*