Дослідження засобів біометричної автентифікації користувачів при використанні хмарних технологій

Виконала студентка ДА-62, Петренко Марія

Дипломний керівник Капшук О.О.

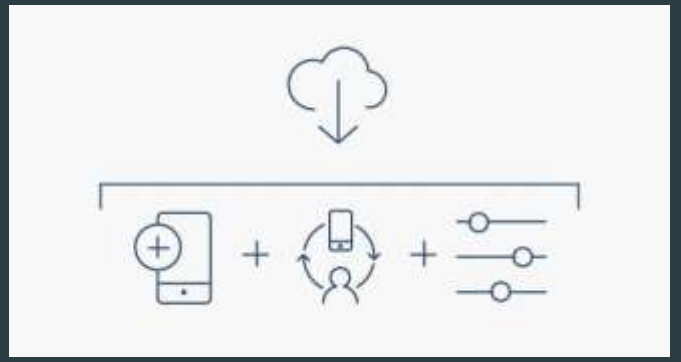
Мета роботи

- Аналіз питань безпеки в хмарних технологіях
- Дослідження засобів біометричної автентифікації в хмарних технологіях
- Порівняльний аналіз засобів біометричної автентифікації в хмарних технологіях, а також відповідні рекомендації на основі цих висновків

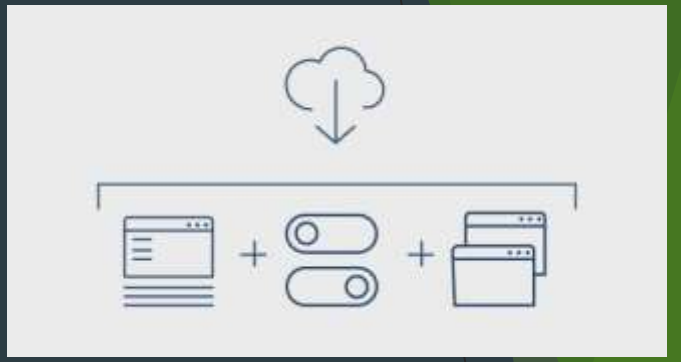
Актуальність

- За останні п’ять років хмарні технології стали однією з IT сфер, що розвивається надто швидко
- До 80% паролів може бути зламані за кілька хвилин.
- Хакери зламали хмарний сервіси, і отримують доступ до паролів, IP-адресів, інформації про здоров'я співробітників і даних, що стосуються бізнесу.
- Хакери намагаються дістати несанкціонований доступ до хмарних сервісів, щоб красти ресурси для добування криптовалюти, а не внутрішню інформацію компаній.

Інфраструктура як послуга (IaaS)
Постачальник надає клієнтам доступ до сховища, мереж, серверів та інших обчислювальних ресурсів в хмарі з оплатою за фактом використання.



Платформа як послуга (PaaS)
Постачальник послуг пропонує доступ до хмарного середовища, в якій користувачі можуть створювати і експлуатувати додатки. Підтримка базової інфраструктури здійснюється постачальником.

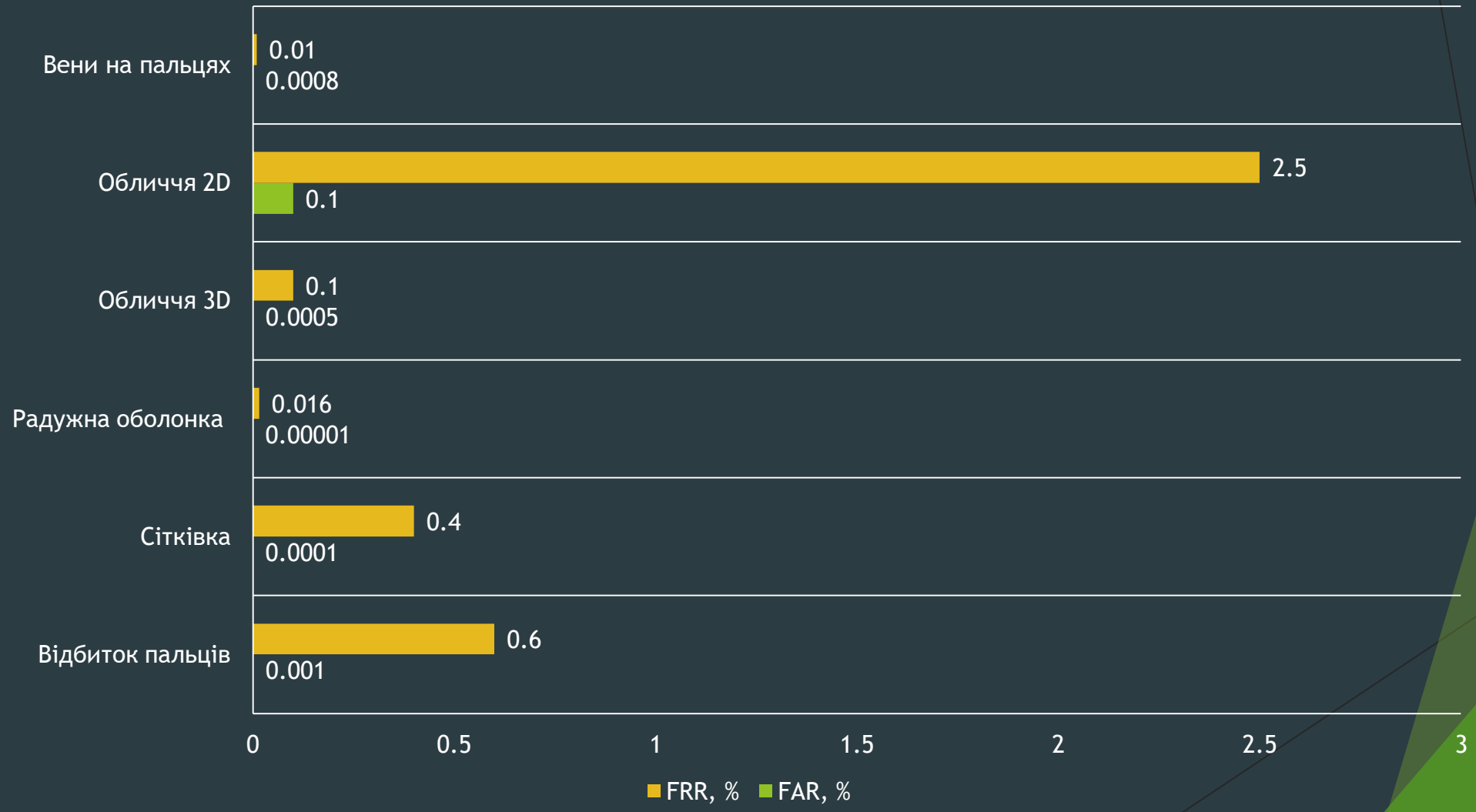


Програмне забезпечення як послуга (SaaS)
Постачальник послуг доставляє програмне забезпечення і додатки через Інтернет. Користувачі підписуються на ПО і отримують до нього доступ через веб-інтерфейс або API вендора.

Засоби біометричної автентифікації в хмарних технологіях

- Сканування відбитку пальця
- Сканування вен пальця
- Сканування долоні
- Сканування обличчя 2D і 3D
- Сканування райдужної оболонки
- Сканування сітківки

Коефіцієнти FAR і FRR для порівняння засобів біометричної автентифікації [1]



Швидкість методів автентифікації

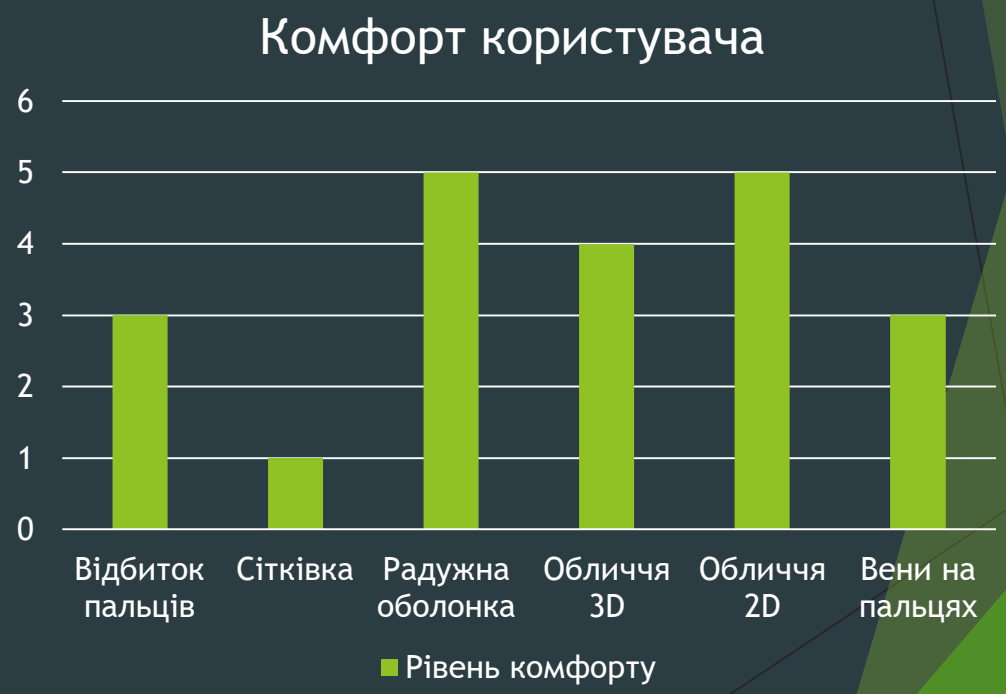
Біометрична система	Швидкість розпізнавання, сек
Відбиток пальця	0,2
Обличчя 2D	0,3
Обличчя 3D	0,6
Вени пальця	< 0,2
Райдужна оболонка	< 0,2
Сітківка	0,8

Біометрична система	Швидкість розпізнавання, шаблони в секунду
Відбиток пальця	300 000
Обличчя 2D	90 000
Обличчя 3D	70 000
Вени пальця	250 000
Райдужна оболонка	100 000
Сітківка	60 000

Біометрична система	Сумарне порівняння швидкості
Відбиток пальця	Висока
Обличчя 2D	Середня
Обличчя 3D	Низька
Вени пальця	Висока
Райдужна оболонка	Висока
Сітківка	Низька

Можливості безконтактності та комфорту методів автентифікації

Біометрична система	Безконтактність
Відбиток пальця	Неможлива
Обличчя 2D	На великій відстані
Обличчя 3D	На невеликій відстані
Вени пальця	Мала відстань
Райдужна оболонка	На середній відстані
Сітківка	Неможлива



Чутливість методів автентифікації до зовнішних факторів і незмінність характеристик методу

Біометрична система	Чутливість
Відбиток пальця	Висока (порізи, вода)
Обличчя 2D	Висока (косметика, пошкодження обличчя, одяг)
Обличчя 3D	Низька
Вени пальця	Середня(пошкодження, хірургічне втручання)
Райдужна оболонка	Середня (пошкодження, хірургічне втручання)
Сітківка	Висока

Біометрична система	Незмінність з часом
Відбиток пальця	Низька
Обличчя 2D	Низька
Обличчя 3D	Висока
Вени пальця	Середня
Райдужна оболонка	Висока
Сітківка	Середня

Фальсифікація методів

Біометрична система	Можливість фальсифікації
Відбиток пальця	Середня
Обличчя 2D	Середня
Обличчя 3D	Дуже низька
Вени пальця	Неможлива
Райдужна оболонка	Практично неможлива
Сітківка	Неможлива

Орієнтовна вартість засобів біометричної автентифікації

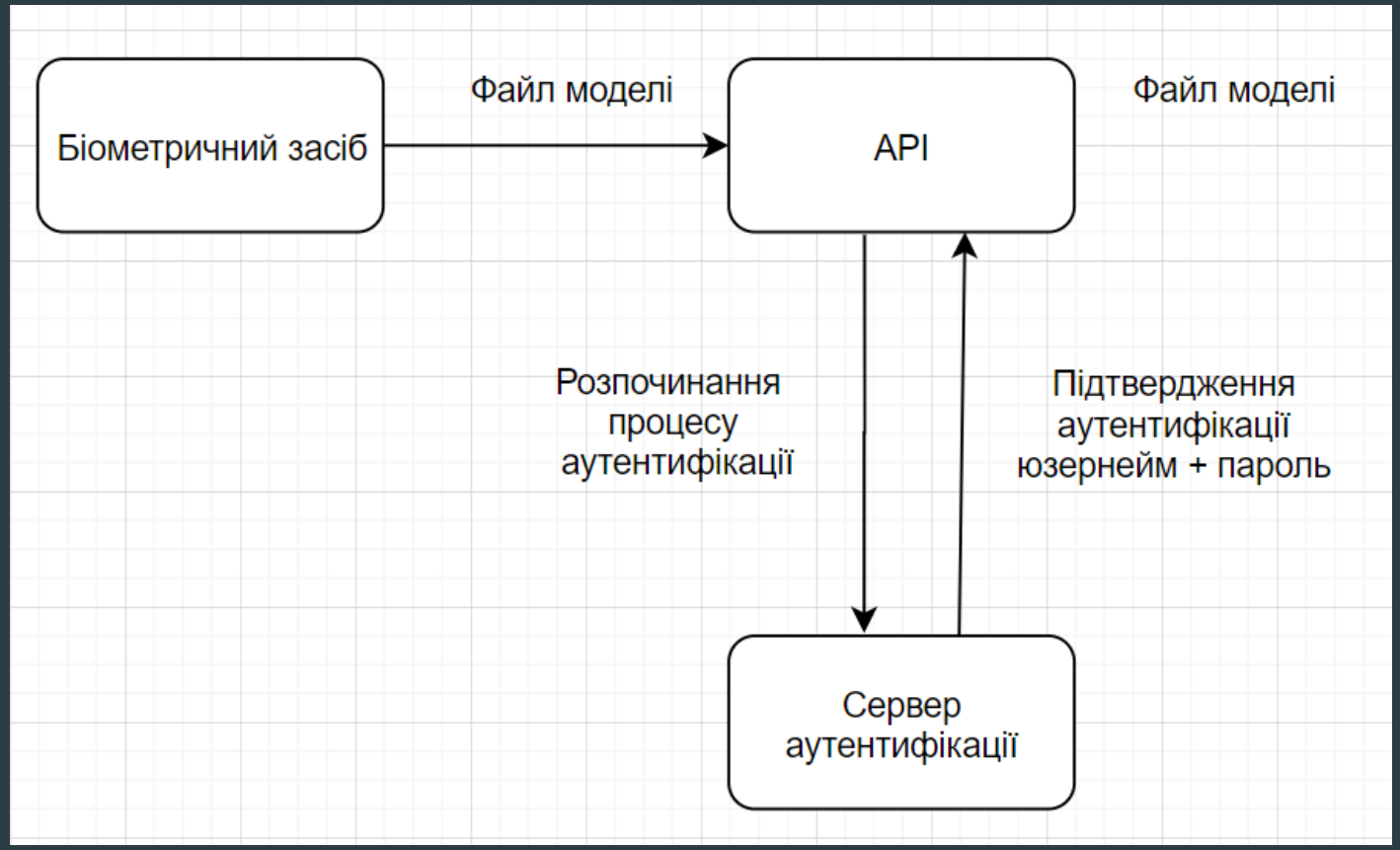
Біометрична система	Статистична вартість
Відбиток пальця	Низька
Обличчя 2D	Середня
Обличчя 3D	Висока
Вени пальця	Середня
Райдужна оболонка	Висока
Сітківка	Висока

Біометрична система	Статистична вартість	Безпека	Доступність на ринку	Безконтактність	Вбудованість
Відбиток пальця	Низька	Середня	Висока	Немає	Присутня
Обличчя 2D	Середня	Середня	Висока	Присутня	Присутня
Обличчя 3D	Висока	Висока	Висока	Присутня	Присутня
Вени пальця	Середня	Висока	Висока	Присутня(не в релеватній відстані)	Відсутня
Райдужна оболонка	Висока	Висока	Середня	Присутня	Присутня(але не розповсюджена)
Сітківка	Висока	Висока	Низька	Відсутня	Присутня(але не розповсюджена)

IaaS – важливий рівень фізичного доступу, найкращим інструментом є сканер вен пальця/руки

PaaS – важливий рівень фізичного доступу, найкращим інструментом є сканер вен пальця/руки, відбиток пальців, обличчя 3D

SaaS – захист програмних додатків, найкращим інструментом є відбиток пальців, обличчя 3D



API встановлює новий сеанс у веб-інтерфейсі для кінцевого користувача, щоб отримати доступ до програми SaaS, до якої йому потрібен доступ, потім API створює та надсилає Ідентифікатор сесії на комп'ютер кінцевого користувача, кінцевий користувач тепер може завантажити цю конкретну програму на основі SaaS на власний комп'ютер та отримати доступ через графічний інтерфейс користувача (GUI) через веб-браузер за власним вибором.

Висновки

- В цілому в дипломній роботі були розглянуті три основні моделі обслуговування хмарних сервісів та як біометрію можна використовувати для захисту кожної з них, як з точки зору фізичного доступу, так і з точки зору логічного доступу. Зроблене припущення методології, яка може захистити хмарну інфраструктуру.

- Хоча для захисту інфраструктури, що базується на хмарі, досі застосовуються інші заходи безпеки (як це було розглянуто раніше), біометрія має одну чітку перевагу перед ними. Це єдиний механізм, який може на 100% підтвердити особистість, оскільки риси є унікальними для кожної людини.

- Але, як і все інше, біометрія не повинна бути єдиною лінією захисту у захисті інфраструктури, заснованої на хмарі. Його слід застосовувати разом з іншими заходами безпеки, щоб створити те, що відоме як мультимодальне рішення безпеки. Це забезпечує реалізацію найвищих рівнів безпеки, оскільки одночасно використовується декілька її шарів.

Дякую за увагу!

Перелік посилань:

1. https://www.biometricupdate.com/
2. https://security-shop.com.ua/biometricheskie-sistemy/