Технічні науки

УДК 004.422.83

Грицай Аліна Юріївна

бакалавр комп'ютерних наук

Національного технічного університету України

«Київський політехнічний інститут імені Ігоря Сікорського»

Грицай Алина Юрьевна

бакалавр компьютерных наук

Национального технического университета Украины

«Киевский политехнический институт имени Игоря Сикорского»

Gritsay Alina

Bachelor of Computer Science of the

National Technical University of Ukraine

«Igor Sikorsky Kyiv Polytechnic Institute»

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ FINGERPRINT ДЛЯ АУТЕНТИФІКАЦІЇ У ВЕБ-ЗАСТОСУНКАХ
ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ FINGERPRINT ДЛЯ АУТЕНТИФИКАЦИИ В ВЕБ-ПРИЛОЖЕНИЯХ
USING FINGERPRINT TECHNOLOGY FOR AUTHENTICATION IN WEB APPLICATIONS

Анотація. *Дана стаття присвячена аналізу та розробці технології Fingerprint, яка реалізує аутентифікацію на основі відбитків пальців.*

Ключові слова: *Fingerprint, Веб-додаток, аутентифікація.*

Аннотация. *Данная статья посвящена анализу и разработке технологии Fingerprint, которая реализует аутентификацию на основе отпечатков пальцев.*

Ключевые слова: *Fingerprint, Веб-приложение, аутентификация.*

Summary. *This article is devoted to the analysis and development of Fingerprint technology, which implements fingerprint authentication.*

Key words: *Fingerprint, Web application, authentication.*

Вступ. 4 млрд населення світу є інтернет-користувачами. Вимогами сучасності у всіх сферах життя стала можливість супроводжувати своє представлення в Інтернеті та можливість надання та отримання онлайн-послуг.

Потік конфіденційної інформації, спровокований онлайн банкінгом та безліччю інших платіжних систем вимагає належного рівня безпеки. Інформація в Інтернеті відтворюється на основі Веб-сайтів, користувачі отримують доступ до послуг після проходження аутентифікації на сайті. Аутентифікація — процес ідентифікації користувача на відповідність і надавання певного рівня доступу до системи. З розвитком біометричних технологій процес аутентифікації значно спростився. Біометрія — це ідентифікація особи за рядом біологічних ознак.

За останні кілька років, спостерігається зростання кількості мобільних пристроїв, обладнаних сканерами відбитків пальців. На відмінну від методів, що використовують паролі, біометричний метод аутентифікації працює на основі біологічних особливостях людини, які неможливо загубити чи викрасти.

Основна частина. При біометричній аутентифікації реальний і пред'явлений ключі порівнюються з можливою похибкою, що обумовлюється заздалегідь і береться за константу. А відхилення обирається щоб зафіксувати оптимальне поєднання цих двох коефіцієнтів:

FAR (False Accept Rate) - коефіцієнт неправильного визначення (нелегальний клієнт авторизувався під ім'ям чужого клієнта).

FRR (False Reject Rate) - коефіцієнт помилкового неузгодження (реальний клієнт не пройшов ідентифікацію).

FAR і FRR визначають у відсотковому інтервалі та значення повинні бути якомога меншими. За нормами біометричної ідентифікації значення має дорівнювати FAR 0,01-0,001% при FRR до 3-5%.

Таблиця 1

Коефіцієнти FAR і FRR для найпопулярніших методів біометричної аутентифікації [1]

Біометрична властивість	FAR	FRR
Сканування обличчя 2D	0,1%	2,6%
Сканування обличчя 3D	0,0004%	0,1%
Сітчатка ока	0,0001%	0,4%
Райдужка ока	0,00001%	0,015%
Відбиток пальця	0,001%	0,6%

Біометричну систему можна поділити на два окремих модулі: ідентифікації та реєстрації. Модуль реєстрації навчає систему уміти розпізнавати конкретного користувача. На цьому етапі датчики зчитують біометричні характеристики користувача і перетворюють ці дані в цифрове представлення. Потрібен окремий модуль для порівняння користувачів з еталонними шаблонами. Введений шаблон порівнюється з еталонним.

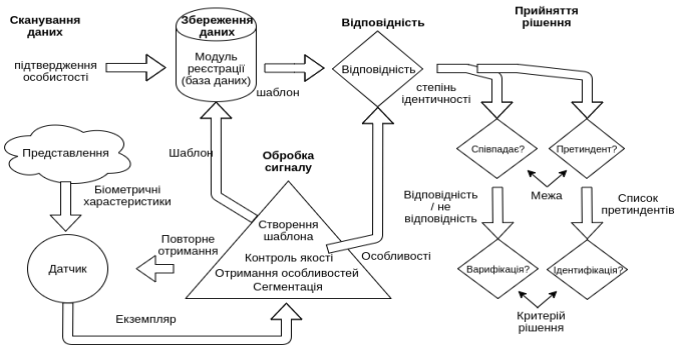

Рис. 1. Загальна схема роботи біометричної системи

Для користувачів також важливі наступні характеристики:

- можливість аутентифікації та ідентифікації;
- складність реалізації системи ідентифікації;
- точність перевірки;

- розмір шаблону;
- комфорт.

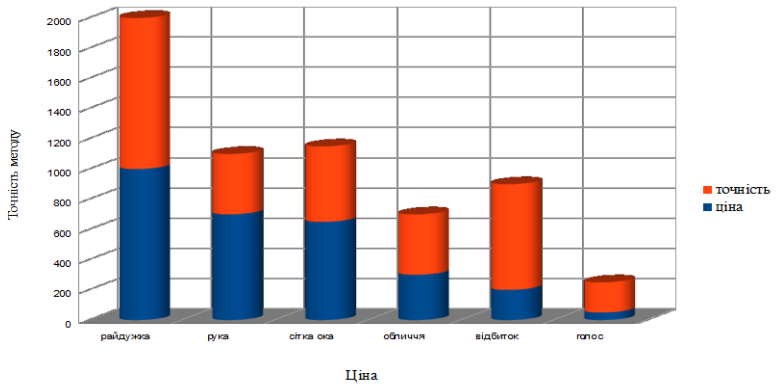

Рис. 2. Співвідношення ціни та якості методів біометричної аутентифікації

На поверхні шкіри пальців є випуклі виступи, що і дозволяють проводити біометричну аутентифікацію. Доведено, що не існує двох людей з двома однаковими відбитками пальця.

Кожен відбиток пальця має глобальні та локальні властивості. Глобальні властивості — це ті, що можливо побачити неозброєним оком: папілярний візерунок; область образу — частина, в якій локалізовано всі ознаки; ядро — центр середини відбитка пальця; точка початку — та частина, де відбувається поділ або з'єднання ліній;

Локальні властивості, мануції — неповторні у кожного відбитка пальця маленькі папілярні лінії, які слугують закінченнями основних, більш товстих ліній.

Розглянемо основні вимоги до відбитків пальців:

- шаблон має бути з 256 рівнями яскравості;
- шаблони зберігаються в не стислому вигляді;
- відбиток має бути повернутий не більше, ніж на 20 градусів.

Для кращої роботи алгоритму зберігають декілька шаблонів відбитка пальця у базі даних. Першочергово слід покращити якість зчитаного відбитку, збільшивши чіткість папіляріїв. Зображення перетворюють в

чорно-біле. Всі ліній деталізують до розміру в 1 піксель. Далі за алгоритмом проводиться зчитування блоків даних. Вся площа ділиться на квадрати 9 на 9 пікселів, опісля знаходить кількість пікселів чорного кольору, що розташовуються коло центра. Таким чином визначаються маніції, чорні пікселі, що розташовуються в центрі.

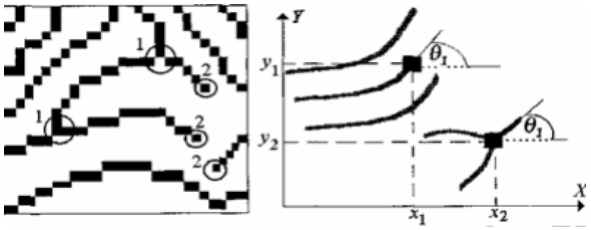

Рис. 3. Визначення муніцій [2]

Після чого муніції детермінуються точками на відрізках координат, а їх напрямки записуються у векторній формі.

$$W(p) = [(x_1,y_1,\theta_1),(x_2,y_2,\theta_2),...(x_p,y_p,\theta_p)], \quad (1)$$

де — p число муніцій.

Загальна формула ідентифікації відбитка пальця:

$$K = D^2\, 100\% / pq\,,$$

де D — кількість муніцій, що однакові;

p - кількість муніцій еталона;

q - кількість муніцій введеного відбитка.

Якщо результат понад 60%, то аутентифікація успішна.

Першого широкого використання сканери набули з виходом на ринок смартфонів iPhone 5s, саме з цього телефону Apple започаткував свою технологію оптичної кнопки під назвою Tuch ID. В сучасних смартфонах використовуються оптичні сканери відбитків пальця. Світлодіодна матриця освічує папілярні візерунки, а світлочуттєві фотодіоди за допомогою мікросхеми роблять знімок. Камера отримує відбитий потік інформації у вигляді сигналу в нижній частині поверхності пристрою, в той час, коли палець доторкається до поверхні. Коли на фотодіоди потрапляє потік світла, вони провокують електричний заряд. В залежності від інтенсивності світла

пікселі групують відбиток пальця.

Перейдемо до програмної реалізації. Для створення системи контролю доступу потрібно реалізувати такі функції модуля:

- Реєстрація відбитків пальців.
- Порівняння відбитків пальців.
- Видалення відбитків пальців.

Для створення системи контролю доступу використаємо сканер відбитків пальців ZFM-20 та спочатку протестуємо його роботу за допомогою Arduino. Adafruit_Fingerprint бібліотека для роботи з дактилоскопічними датчиками на Arduino, вона реалізує взаємодію з сканером пальців та виконує ряд вище вказаних функцій. Для запису відбитків пальців до бази необхідно підключитись до бібліотеки "Adafruit_Fingerprint.h" та "SoftwareSerial.h" [3].

При успішному зчитуванні даних з сенсора у консоль надійдуть повідомлення про вдале зчитування відбитку.

У Веб-застосунках для користувачів обов'язковими вимогами є наявність інтерфейсу та збереження даних користувачів у базі. Слід враховувати відсутність датчика на деяких пристроях та забезпечити можливість аутентифікації користувача іншим способом. Архітектура має містити такі модулі:

- основний модуль аутентифікації користувача з наявністю датчика відбитків пальців у пристрої;
- запасний модуль аутентифікації користувача за допомогою токенів, без використання відбитку пальця.

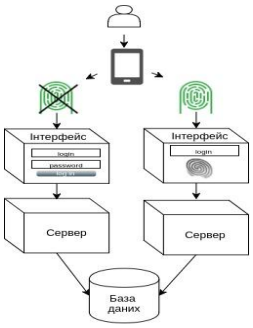

Рис. 4. Архітектура Веб-застосунку з використанням технології Fingerprint

Обидва модулі мають складатися з інтерфейсу, серверної частини та бази даних. Інтерфейс основного модуля, за допомогою датчика відбитку пальця, має містити поле для вводу логіна та поле, що буде показувати процес зчитування відбитка. Після того як користувач введе логін йому необхідно доторкнутися пальцем датчика на своєму пристрої. Далі сканер відскануює відбиток та у вигляді цифрових даних створить шаблон відбитка пальця.

Сервер отримає ці дані в масив. За логіном у базі даних сервер знайде еталон відбитка пальця та порівняє ці два відбитки.

Якщо датчика відбитка пальця не буде виявлено на пристрої, то Веб-застосунок проведе аутентифікацію на базі пароля. Сервер надішле запит до бази даних. За логіном користувача знайде та порівняє отриманий пароль з паролем із бази даних після чого користувач зможе пройти процес авторизації та отримати доступ до своїх даних у Веб-застосунку.

Веб-застосунок має складатись з двох частин: клієнтської частини та сервера. Візуальна частина має представляти собою сторінку в просторі Інтернет для якої буде використано зрозумілі елементи для проходження процесу аутентифікації. Перш за все Веб-застосунок робить перевірку на наявність датчика відбитку пальців. Після чого сервер надає шаблон інтерфейсу відповідно з результатом перевірки на наявність датчика. Для реалізації клієнтської частини використовується JavaScript для взаємодії з користувачем та забезпеченням інтерактивності. Для створення елементів

візуалізації використовується HTML. А для стилізації і покращення візуального сприйняття використовується CSS.

Якщо процес аутентифікації успішний користувач бачить повідомлення про успішність аутентифікації.

У запасному варіанті, якщо датчик не виявлено, користувач побачить перед собою поле для введення логіну, поле для введення пароля та кнопку для підтвердження вводу і надсилання інформації на сервер. Після успішного процесу аутентифікації користувач побачить повідомлення про проходження процесу аутентифікації. В обох випадках при помилці аутентифікації користувачу буде надіслано повідомлення про повторне введення даних та інформацію про помилковість даних.

Для серверної частини вдало підійде Node.js та фреймворк Express. Для реалізації технології Fingerprint було використано FlexCode SDK, він містить достатню кількість інформації та дозволяє реалізувати необхідних функціонал при аутентифікації користувача.

Для збереження інформації про користувачів було обрано базу даних MongoDB. Вона має просту NoSQL структуру, що полегшує її використання, а також це найбільш популярна нереляційних база даних. MongoDB переважає тому що має гнучкий JSON-формат документів.

Реалізація аутентифікації має проводитись за двома варінтами. Перший реалізовує реєстрацію на основі JWT-token, за відсутності сканера відбитків пальців. JSON Web Token (JWT) — JSON-об'єкт, який містить в зашифрованому вигляді всю мінімально необхідну інформацію для аутентифікації і авторизації. Аутентифікація користувача за допомогою JWT-токенів відбувається наступним чином:

- Користувач запитує доступ до сервера (Authorization Server), висилаючи логін і пароль.
- Authorization Server перевіряє валідність користувача і висилає йому access token, який має якийсь expiration date (2 тижні).

- Користувач використовує цей access token для доступу до ресурсів

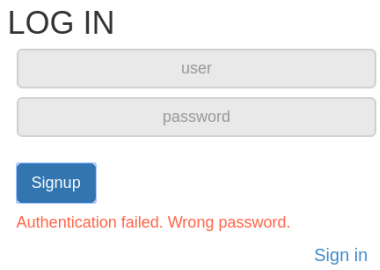

Рис. 5. Реєстрація на основі JWT-token

FlexCode SDK - безкоштовний SDK для розробки програмного забезпечення для відстеження відбитків пальців, призначений для додавання функцій перевірки відбитків пальців. Даний SDK є найбільш придатним для розробки біометричних додатків для входу в систему, зчитує більше 10 відбитків пальців.

SDK працює під Linux, OS X та Windows. Не потребує ніякої інсталяції чи налаштувань на сервері. Функція SDK для перевірки відбитків пальців дозволяє відсканувати відбитки від сканерів та здійснювати перевірку відбитків пальців (відповідність 1: 1). Контроль якості може бути застосований для прийняття лише хороших якісних відбитків пальців від сканерів відбитків пальців.

JavaScript відповідає за клієнтську частину, реакцію на дії користувача та забезпечення інтерактивності.

Рис. 6. Утентифікації за допомогою відбитка пальця

Замість традиційної моделі паралелізму на основі потоків в Node.js використовуються принципи подієво-орієнтованих систем - в порівнянні з підходом «один потік на кожне з'єднання» код виходить простіше і швидше. Node.js став популярний завдяки великому обсягові NPM, а також великій спільноті розробників і можливості використовувати JavaScript на клієнті, на сервері і для розробки інструментів.

Висновки. Сканери відбитків пальців стали досить безпечною альтернативою запам'ятовуванню незліченних імен користувача та паролів, а подальше розгортання захищених мобільних платіжних систем означає, що ці сканери, ймовірно, стануть більш поширеним та найважливішим інструментом безпеки в майбутньому.

Проведене дослідження, в той самий час, показує, що біометричні технології все частіше сприймаються як надійний інструмент аутентифікації в міру того, як люди стають все краще знайомі з використанням цих технологій на своїх пристроях.

Література

1. Ломалкін О. Авторизация в веб: какой она может быть? [Електронний ресурс] / Олексій Ломалкін. – 2008. – Режим доступу до ресурсу: https://habr.com/post/28443. - Дата доступу: 12.04.2018.
2. Виростков Д. Обзор способов и протоколов аутентификации в веб-приложениях [Електронний ресурс] / Дмитро Виростков. – 2015. – Режим доступу до ресурсу: https://dataart.ua/news/obzor-sposobov-i-protokolov-autentifikatsii-v-veb-prilozheniyah/. - Дата доступу: 12.04.2018.
3. Михайлов В. Аутентификация и авторизация в микросервисных приложениях [Електронний ресурс] / В'ячеслав Михайлов. – 2016. – Режим доступу до ресурсу: https://habr.com/company/dataart/blog/311376/. - Дата доступу: 12.04.2018.