

СИСТЕМА АВТЕНТИФІКАЦІЇ КОРИСТУВАЧА В РЕЖИМІ РЕАЛЬНОГО ЧАСУ З МОЖЛИВІСТЮ ШИФРУВАННЯ БІБЛІОТЕКИ СПЕКТОГРАМ

¹ Вінницький національний технічний університет;

Анотація

Запропонована система модуль автентифікації користувача, яка забезпечить можливість автоматичної ідентифікації клієнта в реальному часі, уникнувши зайвого часу на підтвердження особистих даних.

Ключові слова: автентифікація, автентифікація в режимі реального часу, ідентифікація клієнта, розпізнавання голосу, неправомірний доступ, порівняння звуку голосу, шифрування аудіофайлів.

Abstract

The proposed system is a user authentication module, which will provide the possibility of automatic identification of the client in real time, avoiding unnecessary time to confirm personal data..

Keywords: authentication, real-time authentication, customer identification, voice recognition, unauthorized access, voice comparison, encryption of audio files.

Вступ

Системи автентифікації, які використовують останні досягнення технологій, такі як біометрика, двофакторна автентифікація, одноразові паролі, мультифакторна автентифікація, токени та інші методи для підтвердження ідентичності користувачів є стандартними процесами автентифікації користувача, які в більшості випадків базується на простому отриманні конфіденційної інформації та підтвердження для подальшої роботи з клієнтом, тобто в ручному режимі з опитуванням великої кількості питань, зі збільшеним часом автентифікації та незручності, що є основним недоліком в такому процесі [1, 2, 3].

Метою роботи є розроблення система автентифікації користувача в режимі реального часу й можливість зберігання повірених даних в шифрованому вигляді спектограм.

Результати дослідження

Для виправлення недоліків із затратами часу на автентифікацію, запропоновано використання системи, що дозволить автентифікувати користувачів за їх голосом. Зокрема, під час першого звернення до фінансової структури, користувач буде проходити реєстрацію, його голос буде записаний та збережений у системі. Під час наступних звернень користувача, його голос буде порівнюватись з зразком у системі, і агент буде сповіщений, що це аутентичний користувач, а не зловмисник або інша особа, яка не має доступу до даних.

Це дозволить агенту зосередитись на конкретних питаннях або відповідях від клієнта і не витрачати час на ручну автентифікацію. І, оскільки, зберігання мультимедійних файлів, таких як аудіо, є поширеною проблемою коли дані можуть бути скомпроментовані [4]. Тому для захисту цього вмісту пропонується використати шифрування спектрограми голосу.

Отже, алгоритм автентифікації користувача складатиметься з таких етапів:

1. Початок сеансу зв'язку.
2. Старт буферизації звуку (аудіо клієнта буферизується з моменту початку дзвінка).
3. Визначення ідентифікатора клієнта та перевірка чи він зареєстрований в системі.
4. Якщо клієнт не зареєстрований – він автоматично створиться, якщо зареєстрований, продовжаться наступні кроки.

5. Шифрування аудіо файлу у вигляді спектрограми та збереження її у базі даних.
6. Відправка запиту на автентифікацію в програмний модуль (для зареєстрованих попередньо клієнтів). Відправляється весь записаний буфер аудіо.
7. Якщо для автентифікації було не достатньо аудіо – повернеться статус, який покаже, що потрібно більше аудіо клієнта та агент зможе повторити запит пізніше.
8. Порівняння існуючої спектрограми та отриманої.
9. Відправка результату автентифікації агенту.
10. Оновлення метаданих дзвінка, тобто зберігаємо всі отримані результати в журналі.

Висновки

Таким чином, запропонована система автентифікації дозволить користувачу та власнику системи(фінансовій структурі) в автоматичному режимі ідентифікувати клієнтів, з неможливістю скомпроментувати данні злоумисниками та не витрачаючи зайвий час на підтвердження особистих даних.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Аутентификация и авторизация: сравниваем лучшие Identity-провайдеры для реализации Single Sign On. [Електронний ресурс]. Режим доступу: <https://dou.ua/forums/topic/35467/>
2. Захист ваших файлів за допомогою двофакторної автентифікації [Електронний ресурс]. Режим доступу: <https://experience.dropbox.com/uk-ua/resources/what-is-2fa>
3. Authentication and authorization [Електронний ресурс]. Режим доступу: https://vladislavremeev.gitbook.io/qa_bible/seti-i-okolo-nikh/autentifikaciya-i-avtorizaciya-authentication-and-authorization
4. Муляр, І., Ленков, Є., & Солодєєва, Л. (2016). ШИФРУВАННЯ ЗВУКУ МЕТОДОМ ПРЕДСТАВЛЕННЯ ЙОГО У ВИГЛЯДІ СПЕКТРОГРАМИ. Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка, (51), 177–185. вилучено із <https://miljournals.knu.ua/index.php/zbirnik/article/view/148>
5. Albahrani, E.A.; Alshekly, T.K.; Lafta, S.H. A Review on Audio Encryption Algorithms Using Chaos Maps-Based Techniques. J. Cyber Secur. Mobil. 2021, 11, 53–82.

Крайній Євгеній Сергійович — студент групи гр. ЗАКІТР-23м, кафедра автоматизація, комп'ютерно-інтегровані технології та робототехніка. Інформаційні системи і Інтернет речей. Вінницький національний технічний університет, Вінниця, e-mail: gorgbushe@gmail.com.

Кулик Ярослав Анатолійович — к.т.н., доцент кафедри Автоматизації та інтелектуальних інформаційних технологій, Факультет інтелектуальних інформаційних технологій та автоматизації, Вінницький національний технічний університет, Вінниця, e-mail: kulyk.y.a@vntu.edu.ua

Krainii Yevhenii S. — Faculty of Intelligent Information Technology and Automation, Vinnytsia National Technical University, Vinnytsia, Ukraine, e-mail: gorgbushe@gmail.com.

Kulyk Yaroslav A. – Associate Professor of Automation and Intelligent Information Technologies Department, Faculty of Intelligent Information Technology and Automation, Vinnytsia National Technical University, Vinnytsia, e-mail: kulyk.y.a@vntu.edu.ua