УДК 004.4

С. А. Айвазян
Л. М. Куперштейн

ПРОЦЕСИ ФУНКЦІОНУВАННЯ СИСТЕМИ ГОЛОСОВОЇ АВТЕНТИФІКАЦІЇ НА ОСНОВІ ХМАРНИХ ТЕХНОЛОГІЙ

Вінницький національний технічний університет

Анотація
Спроектовано систему голосової автентифікації програмного додатку на основі хмарних технологій. Розпізнавання голосу впроваджено за допомогою інтелектуального хмарного сервісу.
Ключові слова: кібербезпека, автентифікація, двофакторна автентифікація на основі голосу, база даних, хмарний сервіс.

Abstract
A two-factor voice-based authentication system software has been designed. Voice recognition is implemented using an intelligent cloud service.
Keywords: cybersecurity, authentication, two-factor voice-basis authentication, database, cloud service.

Вступ

За сучасних умов інформаційне забезпечення стало важливою областю процесу управління. Передача інформації про стан та діяльність організації на вищий рівень управління та взаємний обмін інформацією між усіма взаємопов'язаними підрозділами організації здійснюється на базі сучасної електронно-обчислювальної техніки та інших технічних засобів зв'язку [1].

На сьогоднішній день використання автентифікації є необхідною мірою захисту будь-якого вебзастосунку, але на жаль, із швидкими темпами розвитку інформаційних технологій, з’являються все нові та нетривіальні шляхи до зламу облікових сторінок користувачів та програмних продуктів в цілому.

Системи автентифікації на основі паролів є більш вразливими, ніж системи, що вимагають декількох незалежних методів, як наприклад – голосова автентифікація [2]. Вона характеризується простотою в застосуванні, відсутністю необхідності використання дорогої апаратури, а також різноманітністю способів формування профілю користувача.

Метою роботи є побудова архітектури системи голосової автентифікації на основі хмарних технологій, що надають можливість використовувати функції розпізнавання голосу.

Технічне проектування системи

Архітектура системи автентифікації на основі голосу складається з декількох підсистем, що відрізняються своїм функціональним призначенням.

Система починає роботу з підсистеми візуалізації, запускаючи графічний інтерфейс та ініціалізуючи дані, пов’язані з коректною роботою програми, взаємодіючи з інформаційною системою і виконуючи підключення до бази даних, в якій зберігаються дані до облікових сторінок користувачів.

Для виконання поставлених задач програма звертається до двох підсистем в архітектурі – «Підсистема реєстрації користувача в системі» та «Підсистема керування», кожна з них безпосередньо звертається до інформаційної підсистеми, щоб отримати інформацію, що вводить користувач, як за допомогою клавіатури, так і за допомогою мікрофону, в залежності від того, яка підсистема виконує свої завдання звернення до бази даних відбувається або з метою читання даних, або з метою запису нового облікового запису. При цьому, зазначається, що персональний комп’ютер користувача завчасно має встановлену звукову карту, мікрофон та підключення до інтернету [3].

При записі «голосового відбитку» програма звертається до віддаленого серверу, що має функцію розпізнавання голосу (далі – розпізнавач), який використовує нейронні мережі для ідентифікації голосу користувача та перевірки на її автентичність до входження в систему, перевірки на відповідність актуального голосу користувача та створеного голосового відбитку – голосового еталону.

Зчитані голосові повідомлення з мікрофона передаються до сервера з розпізнавачем та за допомогою вбудованих алгоритмів підраховує у відсотковому співвідношенні ймовірність факту вимови саме того слова чи фрази, яке передав через мікрофон користувач.

Програмний засіб виконуватиме дві основні функції – створення облікового запису та автентифікація у систему. При виконанні обох функцій, користувач повинен вводити свої дані, зокрема логін, пароль у вікна запиту, записувати «голосовий відбиток» та вимовити секретне слово для подальшої автентифікації в систему.

Програма, в свою чергу, шифруватиме локальні дані і передаватиме їх у базу даних системи автентифікації, передавати «голосовий відбиток» до хмарного сервісу, що виконує завдання розпізнавання голосового повідомлення, виконуватиме операцію читання з бази даних для підтвердження усіх етапів автентифікації та гарантувати ідентифікацію «голосового відбитку» з бази даних та утвореного користувачем [3].

Загальний алгоритм роботи системи автентифікації на основі голосу зображений на рисунку 1.

Рисунок 1 – Загальний алгоритм роботи системи автентифікації на основі голосу

Користувач запускає програму і бачить перед собою меню у формі діалогового вікна з кнопками, що мають назви «створити користувача», «увійти в систему» або «завершити роботу».

1) «Створити користувача»:

a. Користувач вводить логін -> Програма перевіряє чи логін наявний в базі даних, якщо не наявний – продовжує роботу із програмою, інакше користувач повинен придумати інший логін;

b. Користувач вводить пароль -> Програма перевіряє на виконання обов'язкових умов про введення паролю (мінімум 12 символів, хоча б один великий символ, цифра і спеціальний символ), якщо пароль відповідає усім умовам – користувач продовжує роботу з програмою, інакше програма запропонує придумати новий пароль;

c. Користувач повторно вводить пароль -> Програма перевіряє на відповідність пароля до його попереднього введення, якщо паролі еквівалентні – користувач продовжує роботу, інакше програма запропонує написати пароль повторно;

d. Користувач залишає голосовий відбиток -> Запускається мікрофон, програма чекає на вхідні дані з мікрофону протягом певного часу, після отримання даних голосова інформація записується в базу даних, а користувач повертається на головне меню програми.

2) «Увійти в систему»:

a. Користувач вводить логін -> Програма перевіряє чи логін наявний в базі даних, якщо не наявний – продовжує роботу із програмою, інакше користувач повинен придумати інший логін;

b. Користувач вводить пароль -> Програма перевіряє на відповідність пароля до його пароля збереженого в базі даних, якщо паролі еквівалентні – користувач продовжує роботу, інакше програма запропонує написати пароль повторно (у користувача є ще три спроби, при відсутності спроб користувач повертається на головне меню програми);

c. Користувач залишає голосовий відбиток -> Запускається мікрофон, програма чекає на вхідні дані з мікрофону протягом певного часу, після отримання даних голосова інформація перевіряє голосовий відбиток із наявним в базі даних, якщо відсоток автентичності перевищує допустиму норму, то користувач проходить автентифікацію і отримує доступ до свого облікового запису, інакше повертається на головне меню програми.

d. Користувач отримує повідомлення про входження в систему, зокрема в свій обліковий запис.

3) «Завершити роботу»:

a. Користувач натискає на кнопку «Завершити роботу» -> Програма завершує роботу із програмним засобом;

Алгоритм роботи програми у вигляді схеми з розгалуженнями представлений на рисунку 2.

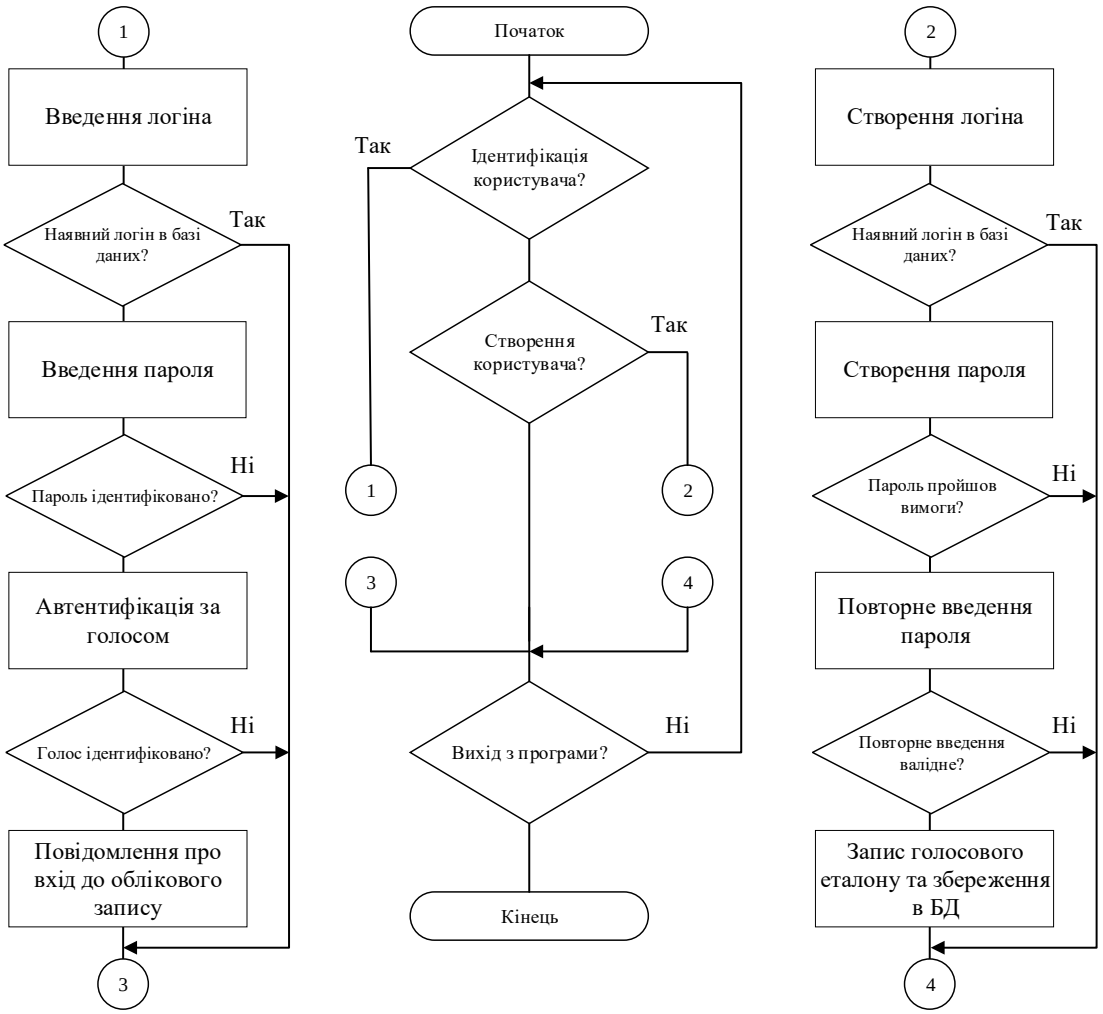

Рисунок 2 – Загальний алгоритм роботи системи автентифікації на основі голосу

Алгоритм порівняння «голосових відбитків» відрізняється способом доступу до бази даних хмарного сервісу, замість запису аудіо-файлу система виконуватиме запит на читання необхідного голосового повідомлення, закріпленого за користувачем, логін якого буде прописано перед виконанням даного алгоритму (рис. 3).

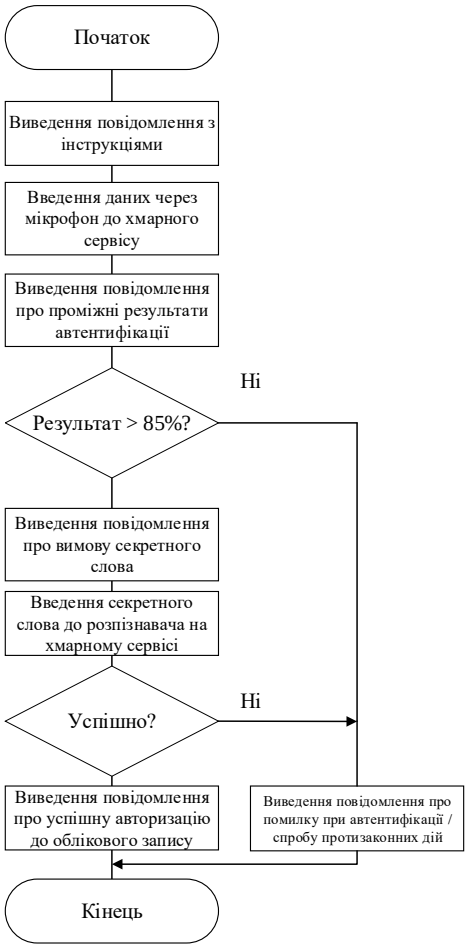

Рисунок 3 – Алгоритм запису «голосового відбитку» до БД хмарного сервісу

Висновки

Розроблено архітектуру та алгоритми функціонування системи голосової автентифікації на основі хмарних технологій.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Методичні вказівки до проведення практичних занять та до виконання самостійної й індивідуальної роботи з дисципліни „Основи науково-дослідної роботи / Укладачі: А. О. Азарова, В. В. Карпінець. – Вінниця: ВНТУ, 2013. – 44 с.
2. Рибченко Д. Є. Аналіз клавіатурного почерку апаратом нечітких множин / Рибченко Д. Є., Іванов А. І. // Технічні засоби конфіденційного зв'язку. – Пенза: ПНІЄІ. – 1996. – Випуск №1. – с. 116-119.
3. Куперштейн Л., Лукічов В., Айвазян С. Система двофакторної автентифікації на основі голосу. [Електронний ресурс]. – Режим доступу: http://www.konferenciaonline.org.ua/arhiv-konferenciy/arhiv-konferenciy11-06-2019 – Назва з екрану.

Айвазян Самвел Арманович — студент групи 1БС-19м, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: 1bs15b.ayvazian@gmail.com

Куперштейн Леонід Михайлович — кандидат технічних наук, доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця

Ayvazian Samvel A. — Student of 1BS-19m, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: 1bs15b.ayvazian@gmail.com

Kupershtein Leonid M. — Candidate of Technical Sciences, Docent of the Information Security department, Vinnytsia National Technical University, Vinnytsia, email: kupershtein.lm@gmail.com