УДК 004

Бадігон В.О, здобувач,
Петросян А.Р., аспірант,
Державний університет «Житомирська політехніка»

РОЗРОБКА БІОМЕТРИЧНОЇ СИСТЕМИ КОНТРОЛЮ ДОСТУПУ НА БАЗІ АРХІТЕКТУРИ EDGE-TO-CLOUD

Сучасні системи контролю доступу все частіше інтегруються з IoT-пристроями [1, 2] та біометричними модулями [3]. Однак більшість існуючих рішень або є закритими пропрієтарними платформами (Kisi), або орієнтовані на B2C-сегмент без належної підтримки біометрії, або вимагають глибокої кастомізації з нуля, наприклад, Home Assistant. Крім того, критичною проблемою залишається захист біометричних даних – передача та зберігання зображень облич створює ризики витоку персональної інформації. Тому актуальним є проєктування власної системи, яка поєднує розподілену обробку даних із вбудованими механізмами конфіденційності.

В основі запропонованого рішення лежить архітектурний підхід Edge-to-Cloud, який передбачає чіткий розподіл функціональних обов'язків між периферійними пристроями та серверною частиною системи. Як показано на діаграмі розгортання (рис. 1), до складу інфраструктури входять інтелектуальні хаби, сервер обробки запитів та база даних. Така організація дозволяє оптимізувати обробку даних і підвищити загальний рівень безпеки. Ключовою особливістю архітектури є винесення процесів біометричної ідентифікації на рівень edge-пристроїв. Smart Hub виконує захоплення зображення, його обробку за допомогою нейромережевих алгоритмів та формування векторного представлення обличчя користувача. При цьому первинні зображення не передаються до мережі, що повністю відповідає принципам концепції Privacy by Design. На сервер передається лише ідентифікатор користувача та ідентифікатор замка, що суттєво знижує ризики компрометації персональних даних.

Серверна частина системи реалізована з використанням модульної архітектури і виконує функції валідації доступу, керування правами та ведення журналу подій. Відповідно до діаграми розгортання, сервер взаємодіє з базою даних, у якій зберігаються списки контролю доступу (ACL), конфігурації пристроїв і журнали аудиту. Перевірка прав доступу здійснюється шляхом виконання цільового запиту до колекції ACL за параметрами userId та lockId. Такий підхід дозволяє отримати рішення про доступ за один запит до бази даних, що є критичним для систем реального часу.

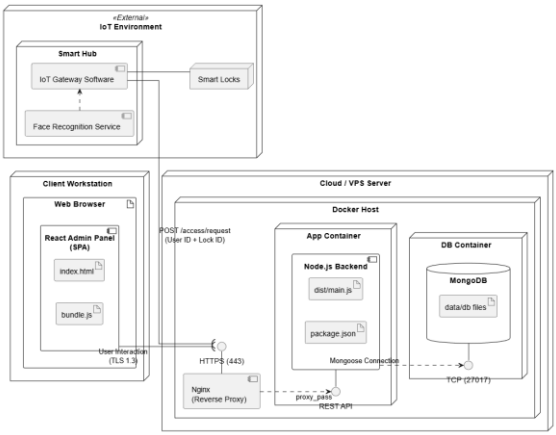

Рис. 1. Діаграма розгортання системи

Безпека системи забезпечується комплексом архітектурних рішень, які також відображено на діаграмі розгортання. Зокрема, реалізовано підхід Zero-Trust, відповідно до якого кожен пристрій автентифікується при кожному запиті до сервера. Додатково застосовано ізоляцію біометричних даних, оскільки сервер не зберігає зображення облич, а оперує лише їхніми векторними представленнями.

Таким чином, запропонована система поєднує розподілену обробку даних, високий рівень безпеки та ефективні механізми управління доступом. Використання підходу Edge-to-Cloud дозволяє досягти балансу між продуктивністю, масштабованістю та захистом персональних даних, що робить систему придатною для впровадження в сучасних корпоративних середовищах.

Список використаних джерел:

1. Ahsan M. S., Pathan A.-S. K. A Comprehensive Survey on the Requirements, Applications, and Future Challenges for Access Control Models in IoT: The State of the Art. *IoT*. 2025. Vol. 6, no. 1. P. 9. URL: https://doi.org/10.3390/iot6010009.

2. Петросян А. Р., Петросян Р. В., Колос К. Р. Розробка платформи віддаленого управління інфраструктурою Інтернет речей. *Технічна інженерія*. 2021. № 1(87). С. 73–80. URL: https://doi.org/10.26642/ten-2021-1(87)-73-80.

3. Biometric-Based Access Control Systems with Robust Facial Recognition in IoT Environments / B. V. Satish Babu et al. *2024 Third International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS)*, Krishnankoil, Virudhunagar district, Tamil Nadu, India, 14–16 March 2024. 2024. URL: https://doi.org/10.1109/incos59338.2024.10527499.