

SECTION 2. COMPUTER SYSTEMS AND NETWORKS, CYBERSECURITY / КОМП'ЮТЕРНІ СИСТЕМИ І МЕРЕЖІ, КІБЕРБЕЗПЕКА

Максим Місюра

Кандидат технічних наук, доцент кафедри комп'ютерних систем, мереж та кібербезпеки
Національний університет біоресурсів і природокористування України, факультет інформаційних
технологій, кафедра комп'ютерних систем, мереж та кібербезпеки, Київ, Україна
ORCID ID 0000-0002-9061-3462
mdm@nubip.edu.ua

Сергій Мамченко

Доктор педагогічних наук, професор, професор кафедри комп'ютерних систем, мереж та
кібербезпеки
Національний університет біоресурсів і природокористування України, факультет інформаційних
технологій, кафедра комп'ютерних систем, мереж та кібербезпеки, Київ, Україна
ORCID ID 0009-0006-8743-5606
s.mamchenko@nubip.edu.ua

ВБУДОВАНА ІОТ СИСТЕМА КОНТРОЛЮ ДОСТУПУ З БІОМЕТРИЧНОЮ АВТЕНТИФІКАЦІЄЮ НА БАЗІ ESP32 ДЛЯ ІНФРАСТРУКТУРИ РОЗУМНИХ БУДІВЕЛЬ

Анотація. У роботі представлено embedded-систему контролю доступу для інфраструктури «розумних» будівель із використанням біометричної автентифікації та інтеграцією до IoT. Апаратною основою є мікроконтролер ESP32 як центральний вузол оброблення даних і мережевої взаємодії; до нього підключено сенсор відбитків пальців (типу R305/AS608), електромеханічний замок і допоміжні модулі. Біометричні дані зчитуються локально, далі здійснюється передача на сервер (через Wi-Fi) для порівняння з еталонними шаблонами і прийняття рішення щодо надання доступу; усі події логуються в базі даних з можливістю віддаленого моніторингу через мобільний застосунок адміністратора. Запропонований підхід поєднує високу зручність користувача з підвищеною надійністю автентифікації порівняно з традиційними методами (ключі, паролі), а також забезпечує масштабованість завдяки IoT-орієнтованим протоколам та гнучким політикам доступу для різних ролей. Новизна полягає в практичній реалізації повного циклу — від сенсора до серверної верифікації та керування виконавчим механізмом — на доступній платформі ESP32 з підтримкою сучасних інтерфейсів, енергозберігаючих режимів і бездротових стеків Wi-Fi/BLE. Додатково обговорюються безпекові аспекти інтеграції (TLS-шифрування трафіку, захист шаблонів, обмеження частоти спроб, 2FA) та сценарії застосування у закладах освіти, офісних просторах, лабораторіях і житлових комплексах. Результати прототипування підтверджують доцільність підходу для побудови безпечних, масштабованих і керованих систем доступу, сумісних із екосистемами smart-building, і окреслюють подальші кроки — використання AI для виявлення аномалій, інтеграцію відеопотоків і впровадження незмінних журналів подій на базі блокчейн-технологій.

Ключові слова: Embedded system; IoT; ESP32; вбудована система; IoT; ESP32; контроль доступу; біометрична автентифікація; розумні будівлі.

1. ВСТУП

1.1. Постановка проблеми

Швидкий розвиток концепції «Розумного будинку» та Інтернету речей (IoT) вимагає впровадження високозахисених та ефективних систем контролю доступу (СКУД). Традиційні СКУД часто страждають від низької надійності, вразливості до компрометації фізичних ключів та складності централізованого моніторингу. Метою даної роботи є розробка гібридної вбудованої IoT-системи контролю доступу з біометричною автентифікацією, яка забезпечує швидку локальну верифікацію та інтегрована з хмарною платформою для віддаленого моніторингу та керування.

1.2. Аналіз останніх досліджень і публікацій

Сфери IoT та біометричної автентифікації (БА) є ключовими для сучасних систем безпеки [1], [2]. Аналіз показує, що IoT-рішення стають галузевим стандартом, забезпечуючи легкість масштабування [3], [4], а ринок систем електронного контролю доступу активно зростає [5]. Серед апаратних рішень, мікроконтролери ESP32 широко використовуються завдяки їхній низькій вартості та вбудованому Wi-Fi, що ідеально підходить для периферійних (Edge) обчислень. Однак більшість існуючих рішень зосереджені або на повністю локальному контролі (без моніторингу), або на повному хмарному контролі (що збільшує затримку). Розроблена система пропонує гібридний підхід, поєднуючи швидкість локальної БА з надійністю хмарного журналу подій.

1.3. Мета публікації

Метою даної публікації є опис розробки та практичної реалізації програмно-апаратної системи контролю доступу. Система базується на біометричній ідентифікації (відбиток пальця) і забезпечує як локальну перевірку на пристрої, так і централізоване логування подій та керування правами доступу через серверну частину.

Для досягнення цієї мети були вирішені наступні завдання:

- Обґрунтовано вибір гібридної архітектури (локальна перевірка, серверне логування).
- Реалізовано апаратну частину на базі мікроконтролера ESP32 та біометричного сенсора.
- Розроблено серверну частину на веб-фреймворку Flask з базою даних PostgreSQL.
- Розгорнуто серверне рішення на хмарній платформі Render для забезпечення глобальної доступності.
- Протестовано систему в реальних сценаріях використання.

2. РЕЗУЛЬТАТИ ТА ОБГОВОРЕННЯ

2.1. Технічна реалізація та архітектура системи

Система функціонує на гібридній архітектурі, що поєднує периферійні обчислення та централізоване хмарне керування для забезпечення високої швидкості та масштабованості.

Локальний IoT-вузол є автономною частиною (Елемент 1), що забезпечує швидкий доступ та фізичний контроль:

- Мікроконтролер ESP32-WROOM-32: Керуюче ядро із вбудованим Wi-Fi. Виконує алгоритми локальної верифікації та керує виконавчим механізмом.
- Біометричний сенсор FPM10A: Відповідає за зчитування, обробку та порівняння відбитка пальця. Підключений до ESP32 через інтерфейс UART.
- Виконавчий механізм (Реле/Замок): Фізичний контроль доступу, керований через лінії GPIO.

Програмна реалізація та синхронізація: Локальна база даних (SQLite) на ESP32 зберігає шаблони відбитків для швидкої автономної верифікації. У разі успішної або невдалої автентифікації, мікроконтролер асинхронно відправляє лог-події через Бездротову мережу (Wi-Fi) та Інтернет (Global Network) (Елемент 2) на Хмарний Сервер.

Хмарна інфраструктура (Елемент 3) є централізованою частиною для адміністрування: Хмарний Сервер: Хостинг (наприклад, Render) для розгорнутого застосунку. Бекенд (Flask/Python): Ядро серверної логіки, що обслуговує REST API для синхронізації логів, обробки запитів керування та взаємодії з інтерфейсом. Централізована База Даних (PostgreSQL): Використовується для надійного зберігання реєстру користувачів та детальних журналів подій доступу (логів).

Користувацький інтерфейс (Елемент 4): Надає адміністраторам засоби для моніторингу та дистанційного керування через Вебінтерфейс (Адміністративна панель), доступний також на Мобільних пристроях.

2.2. Тестування та обговорення результатів

Тестування підтвердило коректну роботу всіх заявлених функцій: локальна ідентифікація успішно розрізняє зареєстрованих та незареєстрованих користувачів, а адміністративна панель коректно відображає журнал подій.

Аналіз показників швидкодії та відмовостійкості. Критична функція локальної ідентифікації виконується приблизно за 1 секунду. Цей показник є важливим, оскільки неблокуючий характер процесу забезпечує високу зручність користувача. Затримка при відправці логу на хмарний сервер склала близько 7 секунд. Ця затримка, пов'язана з особливостями безкоштовного тарифного плану хмарної платформи, є прийнятною, оскільки процес логування відбувається асинхронно і не блокує надання доступу. Реакція системи на команди ручного керування з вебінтерфейсу становить 1-3 секунди. Система довела свою ефективність, надійність та гнучкість в керуванні, поєднуючи швидко локальну верифікацію з перевагами централізованого хмарного моніторингу.

ВИСНОВКИ

У роботі було успішно вирішено завдання розробки та впровадження комп'ютерної системи моніторингу та контролю доступу. Система базується на **IoT-пристроях** та орієнтована на інфраструктуру **«розумних» будівель**.

Підсумки та досягнуті результати: 1. Розроблено вбудовану систему контролю доступу на апаратній платформі мікроконтролера ESP32, яка включає функціональність біометричної аутентифікації для підвищення рівня безпеки та надійності. 2. Створена гібридна архітектура, що поєднує переваги швидкої локальної верифікації безпосередньо на IoT-пристрої з централізованим хмарним моніторингом та керуванням. 3. Забезпечено ефективний механізм управління даними, коли синхронізація журналів верифікації та даних користувачів з локальної бази даних (SQLite) до централізованої (PostgreSQL) відбувається асинхронно (не блокуючи процес надання доступу). 4. Проведена апробація підтвердила, що система є надійною, ефективною та гнучкою у керуванні. Час реакції системи на команди ручного керування через вебінтерфейс становить 1-3 секунди, що відповідає сучасним вимогам до систем контролю доступу.

ПОСИЛАННЯ (ПЕРЕКЛАДЕНІ ТА ТРАНСЛІТЕРОВАНІ)

[1] T. Lynn, S. P. G. Singh, M. O'Connell, and P. Rosati, "The Internet of Things: Definitions, Key Concepts, and Reference Architectures," in *The Cloud-to-Thing Continuum*. Cham: Springer, 2020, pp. 1–25.

[2] A. K. Jain and A. Kumar, "Biometric Recognition: An Overview," in *Second Generation Biometrics: The Future of Biometrics*. New York: Springer, 2012, pp. 3–18.

[3] OptConnect, "Elevating Access Control with IoT," 2023. [Online]. Available: <https://www.optconnect.com/blog/elevating-access-control-with-iot>. [Accessed: Jun. 15, 2025].

[4] A. Salim, S. A. Ghafoor, and K. M. Ghafoor, "IoT-based Smart Access Control Systems: Architecture and Implementation," *Sensors (Basel)*, vol. 20, no. 11, p. 3088, Jun. 2020. doi: 10.3390/s20113088.

[5] SNS Insider, "Electronic Access Control Systems Market to Grow USD 106.68 Billion by 2032," 2025. [Online]. Available: <https://www.snsinsider.com/reports/electronic-access-control-systems-market-1835>. [Accessed: Jun. 15, 2025].

[6] O. B. Prus, "Rozrobka komp'uternoi systemy monitorynhu ta kontroliu dostupu z vykorystanniam IoT prystroiv" ("Development of a computer system for monitoring and access control using IoT devices"), Bachelor's Thesis, Dept. of Computer Systems, Networks and Cybersecurity, Natsionalnyi Universytet Bioresursiv i Pryrodokorystuvannia Ukrainy (National University of Life and Environmental Sciences of Ukraine), Kyiv, Ukraine, 2025.

MINISTRY OF EDUCATION
AND SCIENCE OF UKRAINE

NATIONAL UNIVERSITY
OF LIFE AND ENVIRONMENTAL
SCIENCES OF UKRAINE

FACULTY OF INFORMATION
TECHNOLOGY

МІНІСТЕРСТВО ОСВІТИ
І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
БІОРЕСУРСІВ І
ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ
ТЕХНОЛОГІЙ

PROCEEDINGS

XIII International scientific
and practical conference

**GLOBAL AND
REGIONAL PROBLEMS OF
INFORMATIZATION IN
SOCIETY AND
NATURE USING
'2025**

13-14 November 2025

Kyiv, NULES of Ukraine

Kyiv 2025

МАТЕРІАЛИ

XIII Міжнародної науково-
практичної конференції

**ГЛОБАЛЬНІ ТА
РЕГІОНАЛЬНІ ПРОБЛЕМИ
ІНФОРМАТИЗАЦІЇ В
СУСПІЛЬСТВІ І
ПРИРОДОКОРИСТУВАННІ
'2025**

13-14 листопада 2025 року

Київ, НУБіП України

Київ 2025

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ
І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

МАТЕРІАЛИ

XIII Міжнародної науково-практичної конференції

ГЛОБАЛЬНІ ТА РЕГІОНАЛЬНІ ПРОБЛЕМИ ІНФОРМАТИЗАЦІЇ В СУСПІЛЬСТВІ І ПРИРОДОКОРИСТУВАННІ '2025

13-14 листопада 2025 року

Київ, НУБіП України

Київ 2025

УДК 004

Рекомендовано до друку вченою радою факультету інформаційних технологій Національного університету біоресурсів і природокористування України (протокол № 4 від 18.12.2025).

Укладач: д.т.н., доцент Шкарупило В.В.

Збірник матеріалів XIII Міжнародної науково-практичної конференції "Глобальні та регіональні проблеми інформатизації в суспільстві і природокористуванні '2025", 13–14 листопада 2025 року, НУБіП України, Київ. – К.: НУБіП України, 2025. – 206 с.

Відповідальність за зміст публікацій несуть автори.

© Національний університет біоресурсів
і природокористування України, 2025