Реалізація. Підсистема — частина мікросервісної архітектури OwlView (12 Docker-контейнерів, Flask, React 18, PostgreSQL 15, Redis, Vault). Криптографія — на бібліотеках cryptography і pycryptodome; блокчейн і Merkle-перевірка — у back/blockchain. Працездатність підтверджена 312 автоматизованими тестами (167 pytest + 145 vitest, усі passed) та статичним аналізом SonarQube.

Реалізовано інтегрований механізм, який одночасно забезпечує анонімність респондента, неможливість повторного голосування, верифіковану цілісність агрегату й індивідуальну Merkle-перевірку голосу за O(log n). Схема відсутня у комерційних аналогах і відповідає ст. 25 GDPR «Privacy by Design». Перспективи — zk-SNARK і формальна верифікація в Tamarin Prover.

1. Chaum D. Blind Signatures for Untraceable Payments. Advances in Cryptology: Proceedings of CRYPTO ’82. New York: Plenum Press, 1983. P. 199–203.
2. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. URL: https://bitcoin.org/bitcoin.pdf (дата звернення: 10.05.2026).
3. Barker E. Recommendation for Key Management: Part 1 – General. NIST SP 800-57 Pt. 1, Rev. 5. Gaithersburg: NIST, 2020. 171 p.
4. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27.04.2016 (GDPR). Official Journal of the EU. 2016. L 119. P. 1–88.
5. Merkle R. C. A Digital Signature Based on a Conventional Encryption Function. Advances in Cryptology — CRYPTO’87. LNCS, vol. 293. Berlin: Springer, 1988. P. 369–378.

Аутентифікація користувача на основі тактильних параметрів динаміки натискань клавіш

УДК 004.056

Недвига Є.В., Сиропятов О.А.

Національний університет «Одеська політехніка», 10328108@stud.op.edu.ua, o.a.syropiatov@op.edu.ua

Вступ. Зростання кібератак (session hijacking, credential stuffing) виявило вразливість традиційних парольних механізмів та статичних методів біометрії. Безперервна поведінкова біометрія на основі динаміки натискань клавіш (keystroke dynamics) набуває значення. Класичні підходи із часовими характеристиками (dwell time, flight time) мають обмежену стійкість до імітації та replay-атак. Інтеграція тактильних параметрів (keystroke pressure, pressure profile) підвищує розрізнювальну здатність, оскільки силові показники менш підвладні свідомому контролю. Поширення сенсорних інтерфейсів (Force Touch, Android Pressure API) відкриває нові можливості для пасивної верифікації. Вимоги GDPR та Закону України «Про захист персональних даних» вимагають необоротних перетворень біометричних даних.

Мета роботи. Проєктування та програмна реалізація веб-застосунку для безперервної аутентифікації користувачів, що поєднує часові та тактильні параметри динаміки натискань з метою підвищення точності розпізнавання,

забезпечення стійкості до атак та відповідності стандартам захисту біометричної інформації.

Архітектура та методи реалізації. Система побудована на клієнт-серверній архітектурі з використанням Docker Compose для відтворюваності: клієнтська частина реалізована на React 18 + TypeScript + Vite (збір подій через Pointer Events API та KeyboardEvent, передача через HTTPS), серверна — на Python 3.11 + FastAPI + uvicorn, а сховище даних — на PostgreSQL 16 + SQLAlchemy 2.0. Для верифікації застосовано гібридну модель машинного навчання: SVM з RBF-ядром для швидкої перевірки (10–30 подій), LSTM-мережу (PyTorch 2.4+) для continuous authentication та Isolation Forest для liveness detection. Захист забезпечується через cancelable biometrics (bio-hashing) для проєктування векторів у захищений простір, шифрування AES-256-GCM, ротацію ключів та використання session_id + nonce + таймстампів для протидії replay-атакам. Архітектура повністю відповідає принципам privacy-by-design, стандартам ISO/IEC 24745 та нормам GDPR.

Експериментальні дослідження та результати. Тестування проводилося на 25 сеансах набору тексту тривалістю від 40 до 180 секунд і включало реєстраційні сесії, верифікаційні сесії того самого користувача та імітацію зловмисника. Попередня обробка даних охоплювала медіанну фільтрацію викидів, min-max нормалізацію та формування векторів ознак, а верифікація здійснювалася через косинусну подібність із порогом 0.92. Результати показали, що інтеграція тактильних параметрів знижує коефіцієнт рівної ймовірності помилки (EER) на 45% (до рівня 4.8%), при цьому FAR = 0%, а FRR = 10%. Забезпечено високу стійкість системи: всі replay-атаки (20 спроб) були відхилені, спроби синтезу послідовностей (15 спроб) виявлені, спроби enrollment poisoning заблоковані, витік шаблонів унеможливлено, а side-channel атаки нейтралізовано.

Висновки. Розроблений механізм підтвердив практичну доцільність комбінованого використання часових і тактильних параметрів для безперервної аутентифікації у веб- та мобільних середовищах. Досягнуті показники (EER ≈ 4.8%, FAR = 0%) та висока стійкість до атак (replay, spoofing, poisoning) роблять рішення перспективним для інтеграції в системи мобільного банкінгу, VPN-шлюзи та електронні державні чи корпоративні сервіси. Система повністю відповідає регуляторним вимогам завдяки застосуванню скасовуваної біометрії, шифрування та концепції мінімізації даних. Поточні обмеження рішення включають залежність від якості сенсорів пристроїв, відсутність адаптивного оновлення шаблонів та обмежену вибірку користувачів. Подальший розвиток проєкту передбачає впровадження динамічного оновлення профілю, розширення спектра ознак, використання повноцінної LSTM-мережі для continuous verification та проведення масштабних тестувань на гетерогенних пристроях.

1. Shadman R. et al. Keystroke Dynamics: Concepts, Techniques, and Applications // ACM Computing Surveys. 2024. Vol. 56, iss. 8.
2. ISO/IEC 24745:2011 Information technology – Security techniques – Biometric information protection. Geneva : ISO, 2011.

3. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI (зі змінами).
4. Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation). 2016.
5. Kotani K., Horii K. Evaluation on a keystroke authentication system by keying force // Behaviour & Information Technology. 2005. Vol. 24, iss. 4. P. 289–302.

Застосування архітектури нульової довіри для керування доступом у гетерогенних мережах IoT

УДК 004.056:004.7

Антон Нікітін[1], Сергій Зибін[2]

Державний університет інформаційно-комунікаційних технологій,
[1]a.nikitin@duikt.edu.ua, [2]zysv@ukr.net

Розвиток та впровадження гетерогенних мереж Інтернету речей (IoT) у критичні інфраструктури та кіберфізичні системи актуалізує питання забезпечення їх стійкості до кібератак, особливо в умовах конвергенції IT/OT-технологій [1, 3]. Специфіка даних мереж полягає у великій кількості вузлів із різними обчислювальними можливостями, високій динаміці зміни топології, саме у випадку IT-мереж та інфраструктур, та, що найважливіше, відсутності чітко визначеного мережевого периметра.

Традиційні моделі керування доступом, такі як дискреційна (DAC), мандатна (MAC), рольова (RBAC) або атрибутна (ABAC), розроблялися переважно для статичних IT-інфраструктур із концепцією довіреного внутрішнього середовища, так званого периметрового підходу. У контексті гетерогенних мереж IoT ці класичні підходи демонструють ряд суттєвих недоліків, оскільки вони не здатні швидко адаптуватися до динамічних змін контексту середовища та є критично вразливими до внутрішніх загроз [1, 2]. У випадку успішної компрометації одного легітимного вузла зловмисник отримує можливість безперешкодно здійснювати бокове переміщення всередині мережі (Lateral Movement).

З огляду на зазначені обмеження, виникає об'єктивна необхідність конвергенції парадигм безпеки IoT та принципів нульової довіри [2]. Найбільш перспективним напрямком є застосування архітектури нульової довіри (Zero Trust Architecture, ZTA), базовий принцип якої – «ніколи не довіряй, завжди перевіряй» – сформульовано у концептуальних стандартах безпеки, таких як NIST SP 800-207 [4]. Це дозволяє нівелювати загрози від скомпрометованих пристроїв шляхом запровадження механізмів мікросегментації та безперервної автентифікації кожної транзакції. Проте, безпосереднє перенесення класичних механізмів ZTA на гетерогенні середовища IoT ускладнене через обмеженість обчислювальних ресурсів, наприклад, у кінцевих сенсорів, датчиків, IP-камер та таких пристроїв як актуатори [1, 4].

З огляду на це, метою дослідження є підвищення рівня захищеності гетерогенних мереж IoT шляхом розробки адаптивного методу керування доступом на основі концепції нульової довіри. Для досягнення цієї мети