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

пропонується концептуальна модель методу адаптивного керування доступом, що базується на двоетапному оцінюванні рівня довіри (Trust Score) до вузлів гетерогенної мережі IoT. На першому (проактивному) етапі, під час ініціалізації пристрою в мережі, здійснюється первинна перевірка автентичності суб'єкта (Device Posture) шляхом валідації легковагових ідентифікаційних токенів, що мінімізує початкові обчислювальні витрати. Другий (реактивний) етап передбачає безперервний динамічний моніторинг поведінки вузла під час сесії, який реалізується на рівні граничних вузлів (Edge nodes) або маршрутизаторів без залучення додаткових агентів на самих IoT-пристроях.

Основний фокус методу зосереджено на аналізі мережевих метрик взаємодії, які розподілено на три групи: просторові (відповідність зв'язки IP/MAC, легітимність використовуваних мережевих портів та репутація зовнішніх IP-адрес призначення); об'ємно-часові (інтенсивність запитів, обсяг корисного навантаження у пакетах, часові проміжки активності); транзакційні (співвідношення вхідного й вихідного трафіку Tx/Rx, частота скинутих або невдалих спроб з'єднання).

Наукова новизна запропонованого рішення полягає у відмові від ресурсоємних криптографічних агентів на користь двоетапної оцінки довіри з фокусом на безагентний моніторинг мережевих метрик [1, 4]. Для повноцінної реалізації методу планується здійснити наступні завдання: формалізувати математичний апарат обчислення вектора довіри, розробити алгоритми динамічної сегментації та провести імітаційне програмне моделювання системи на рівні мережевих вузлів.

Висновки та очікувані результати. Запропонована концептуальна модель є теоретичним підґрунтям для безпечної інтеграції Zero Trust в IoT. Кінцевим очікуваним результатом є розроблена програмна імітаційна модель методу адаптивного керування доступом (прототип рішення). Її практичне впровадження дозволить автоматично виявляти поведінкові аномалії вузлів та ізолювати скомпрометовані пристрої, що гарантовано підвищить рівень захищеності IoT-інфраструктур від внутрішніх загроз.

1. Al-Tamimi S., Al-Haija Q. A., Alrawashdeh K. Zero-Trust Architecture for Securing Internet of Things (IoT) Networks: A Review. *2024 5th International Conference on Communications, Information, Electronic and Energy Systems (CIEES)*. – 2024. – P. 1–6. URL: https://doi.org/10.1109/ciees62939.2024.10811176 (дата звернення: 16.05.2026).
2. Wehbe M., Bobelin L. Converging Zero Trust and IoT Security: A Multivocal Literature Review. *arXiv preprint arXiv:2604.24205*. – 2026. URL: https://arxiv.org/abs/2604.24205 (дата звернення: 16.05.2026).
3. Slatvinska V., Bevza V. Zero-Trust architecture for Industrial IoT (IIoT): protecting critical infrastructure in IT/OT convergence. *Scientific papers of Donetsk National Technical University. Series: "Computer engineering and automation"*. – 2026. – № 6(38). – P. 73–80. URL: https://doi.org/10.32782/2786-9024/v4i6(38).359304 (дата звернення: 16.05.2026).

4. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture. NIST Special Publication 800-207. Gaithersburg: National Institute of Standards and Technology, 2020. 59 p. URL: https://doi.org/10.6028/NIST.SP.800-207 (дата звернення: 16.05.2026).

Забезпечення автономності та цілісності даних у мобільних системах управління ремонтними роботами.

УДК 621.395.7 (043.2)

Назар Огінський[1]

Тернопільский національний технічний університет імені Івана Пулюя,
[1]nazar_ohinskyi0706@tntu.edu.ua

Сучасна практика менеджменту в будівництві потребує використання спеціалізованих цифрових інструментів, що гарантують конфіденційність розрахунків та стійкість комерційної інформації до зовнішніх загроз безпеці даних. Проблема ефективного супроводу ремонтних робіт полягає у відсутності зручних інструментів для точних обчислень, а також у ризиках використання хмарних сервісів, що можуть призвести до витоку персональної фінансової інформації [1]. Більшість існуючих рішень вимагають постійної синхронізації, що робить дані вразливими до перехоплення у відкритих мережах.

Метою дослідження є проєктування та розробка автономного мобільного застосунку для автоматизації обчислення площ приміщень та формування кошторисів. Актуальність роботи зумовлена необхідністю мінімізації помилок при ручних розрахунках та потребою у конфіденційному інструменті, який забезпечує повний контроль над даними без залучення сторонніх серверів.

Наукова новизна полягає у розробці моделі автономного функціонування прикладного програмного забезпечення, яка базується на принципах ізоляції фінансових обчислень у локальному середовищі мобільної ОС для мінімізації ризиків перехоплення та витоку комерційної інформації. На відміну від аналогів, запропоновано модель локального збереження даних, яка виключає ризики несанкціоного доступу до інформації у хмарних сховищах.

Для реалізації системи обрано мову Kotlin та фреймворк Jetpack Compose [2]. Програмна архітектура побудована на патерні MVVM, що дозволило ізолювати логіку обчислень від інтерфейсу. Розрахунковий модуль автоматизує визначення необхідних для роботи параметрів об’єкту. Локальне збереження даних реалізовано за допомогою бібліотеки Room на базі SQLite, що гарантує автономність роботи та швидкість доступу до інформації. Цей підхід забезпечує цілісність даних та захист від мережевих загроз, оскільки всі дані обробляються виключно на пристрої [3]. Розроблено каталог робіт, який дозволяє гнучко налаштовувати фінансові параметри проекту в ізольованому середовищі.

Розроблений мобільний застосунок забезпечує автоматизацію основних етапів супроводу ремонтних робіт, поєднуючи зручність інтерфейсу з принципами безпечного збереження даних. Отримані результати підтверджують ефективність локальних баз даних для вирішення прикладних задач будівельної інженерії, гарантуючи приватність фінансових розрахунків.