

DOI: [https://doi.org/10.25140/2411-5363-2025-2\(40\)-303-311](https://doi.org/10.25140/2411-5363-2025-2(40)-303-311)

УДК 004.738.5

Анна Миколаївна Усік¹, Володимир Вікторович Казимир²¹асистент кафедри інформаційних та комп'ютерних систем

Національний університет «Чернігівська політехніка» (Чернігів, Україна)

E-mail: usik18@gmail.com. ORCID: <https://orcid.org/0000-0003-4965-6863>. ResearcherID: E-2911-2019²доктор технічних наук, професор кафедри інформаційних та комп'ютерних систем

Національний університет «Чернігівська політехніка» (Чернігів, Україна)

E-mail: vykazymyr@gmail.com. ORCID: <https://orcid.org/0000-0001-8163-1119>. ResearcherID: Q-2925-2016

ПОКАЗНИКИ ЕФЕКТИВНОСТІ ПЕРСПЕКТИВНОГО ОЦІНЮВАННЯ СИСТЕМ ІНТЕРНЕТУ РЕЧЕЙ

На основі принципів системного підходу та технічного аналізу в роботі представлено метод перспективного оцінювання ефективності функціонування систем Інтернету речей (IoT) у контексті «розумного дому». Запропоновано узагальнений прогностичний підхід до визначення основних техніко-експлуатаційних показників ефективності таких систем, зокрема затримки передачі даних, надійності, масштабованості, енергоспоживання та безпеки. Визначено критерії стабільної та якісної роботи IoT-систем і наведено приклад їх застосування для оцінювання типових сценаріїв створення IoT-системи «розумного дому».

Ключові слова: Інтернет речей; ефективність; техніко-експлуатаційні показники; розумний дім; надійність; оперативність; енергоспоживання, перспективне оцінювання.

Табл.: 2. Бібл.: 26.

Актуальність теми дослідження. Сучасний світ дедалі більше інтегрує цифрові технології у всі сфери життя — від побуту до промисловості. Інтернет речей (IoT) є ключовим напрямом цієї трансформації, оскільки дозволяє створювати інтелектуальні системи, здатні в режимі реального часу збирати, передавати та аналізувати дані. У зв'язку з цим особливої актуальності набуває дослідження ефективності IoT-систем. Оцінка таких систем за технічними та економічними показниками дозволяє забезпечити надійність, безпеку, масштабованість і енергоефективність в умовах зростання кількості підключених пристроїв. Ця тема є актуальною для галузей комп'ютерної інженерії, телекомунікацій, автоматизації, медицини та смартінфраструктури, де використання IoT має стратегічне значення.

Постановка проблеми. Зі зростанням кількості пристроїв у IoT-системах з'являються нові виклики, пов'язані з необхідністю забезпечення їх стабільної роботи, швидкої реакції, енергоефективності та захисту інформації. З огляду на складність розподілених IoT-систем, виникає потреба у нових підходах до їх проєктування, оцінки та керування. Одним із таких підходів є використання когнітивних мап для побудови дорожніх карт розвитку систем, що дозволяє формалізувати знання експертів і приймати зважені рішення [1]. Водночас відсутність уніфікованого підходу до перспективного оцінювання IoT-систем як на етапі проєктування, так і в процесі експлуатації, ускладнює їх впровадження та масштабування в критично важливих сферах. Вирішення цієї проблеми є необхідним для підвищення надійності IoT-рішень, особливо в контексті їх використання у системах реального часу [2; 3].

Аналіз останніх досліджень і публікацій. Питання ефективності IoT-систем розглядаються в роботах IEEE, ITU та IETF, присвячених стандартизації, де визначаються допустимі пороги затримки, надійності, пропускну здатності тощо. Зокрема, у дослідженнях щодо протоколів MQTT, CoAP, Zigbee [4; 5; 6] акцентується увага на затримках і надійності передачі даних. У публікаціях компаній Google (Nest), Amazon (Alexa), Xiaomi та Philips Hue зазначено, що для комфортної взаємодії з користувачем затримка не повинна перевищувати 100 мс [7; 8].

Перспективне оцінювання ефективності IoT-систем потребує не лише класичних техніко-експлуатаційних показників, а й інтеграції формальних моделей, когнітивних критеріїв і досвіду користувача. Огляд сучасних досліджень дозволяє виокремити кілька ключових підходів:

1. Формалізовані архітектурні моделі - El-Dosuky та ін. [3] запропонували аналітичну модель IoT-систем, що враховує архітектуру, обрані технології і протоколи для оптимізації продуктивності. Такі моделі дозволяють передбачати узгодженість параметрів: затримку, пропускну здатність, енергоспоживання.

2. Систематичний огляд драйверів ефективності - Shukla та ін. [8] провели систематичний огляд метрик ефективності IoT — latency, throughput, reliability — аналогічно до сучасних вимог у різних прикладних сценаріях.

3. Оцінювання на основі метрологічного підходу - Donatien Koulla Moulla та ін. [9] провели вимірювання 158 IoT-рішень із погляду метрології — надійності, безперервності, безпеки та якості обслуговування. Такий підхід дозволяє стандартизувати оцінювання IoT-рішень у міжгалузевому масштабі.

4. Оцінювання з урахуванням досвіду користувача – згідно з дослідженням Ruoqi Han та ін. [10] показали, що UX-ключові показники є важливими для оцінювання IoT-екосистем з урахуванням рівня інтеграції користувачів/платформ. Аналогічно, дослідження 2024 р. [11] виокремило 43 показники QoS, орієнтованих на забудовників і користувачів IoT-середовищ.

5. Інтеграція стандартів у промисловому IoT - дослідження Industrial IoT [12] акцентує увагу на перспективі інтеграції стеків протоколів та необхідності стандартизації при створенні міжсистемних рішень, де оцінювання ефективності має включати міжплатформену сумісність і надійність компонентів.

Крім того, до ключових трендів перспективного оцінювання IoT систем належать:

- Перехід до формальних моделей для перевірки на різних рівнях IoT-структури — такі моделі, зокрема на основі E-net, дозволяють формалізувати взаємозв'язки між подіями, процесами й об'єктами системи [2; 4; 8];

- Інтеграція когнітивного моделювання (ROI) – розробка дорожніх карт розвитку з урахуванням взаємозв'язків між компонентами екосистеми IoT є перспективним напрямом, зокрема через ECM/CM (Cognitive Mapping) [1];

- Орієнтація на досвід користувача через UX-аналіз і показники [10; 11];

- Включення метрик роботи в IIoT (Industrial Internet of Things - промисловий Інтернет речей.), сумісності стеків, обчислень на краю (edge computing - підхід до обробки даних, за якого обчислення виконуються безпосередньо біля джерела даних, а не в центральному хмарному центрі), що дозволяє зменшити навантаження на хмару і забезпечити обробку в реальному [6; 12; 13].

Виділення недосліджених частин загальної проблеми. Хоча окремі показники ефективності IoT-систем добре досліджені, у наукових роботах недостатньо уваги приділено систематизації цих параметрів для перспективного оцінювання становлення та розвитку таких систем. Відсутність комплексного підходу, що охоплює як технічні, так і енергетичні та безпекові показники, ускладнює об'єктивне порівняння і вибір оптимального IoT-рішення для конкретної сфери застосування.

Мета дослідження. Метою цієї роботи є формалізація та узагальнення ключових показників ефективності IoT-систем, що дозволяє здійснювати якісну оцінку їхнього розвитку в різних сферах застосування. Досягнення цієї мети передбачає вирішення таких задач:

- виокремлення основних технічних метрик,
- аналіз їхніх типових значень і порогів для реальних систем,
- прикладна інтерпретація на основі сценарію «розумного дому».

Кінцевий результат – структурована модель оцінювання, що може бути використана як основа для проектування або вдосконалення IoT-систем.

Виклад основного матеріалу. Системи Інтернету речей (IoT) характеризуються великою кількістю взаємопов'язаних пристроїв, які збирають, передають і обробляють дані в режимі реального часу. Для оцінки їхньої ефективності використовуються специфічні показники, що охоплюють як технічні, так і економічні аспекти, визначені насамперед серією стандартів:

- **IEEE 802.15.4** — стандарт бездротового обміну даними для сенсорних мереж [14];
- **IEEE 2413-2019** — архітектура Інтернету речей [15];
- **ISO/IEC 30141:2018** — довідкова архітектура IoT [16];
- **IETF RFC 7252** — специфікація CoAP [17];
- **IETF RFC 8967** — специфікація MQTT v5.0 [18];
- **ITU-T Y.2060** — загальна модель і термінологія IoT [19];
- **ITU-T Y.4208** — міжмережевість IoT [20];
- **ISO/IEC 25010:2011** — модель якості ПЗ (надійність, доступність тощо) [21];
- **ISO/IEC 27701:2019** — розширення ISO/IEC 27001 щодо конфіденційності [22];
- **ISO/IEC 29192** — стандарти криптографії для обмежених пристроїв [23];
- **ISO/IEC 17025:2017** — вимоги до калібрування та достовірності вимірювань [24].

Відповідно до перелічених стандартів, а також практик впровадження показники ефективності IoT-систем можуть бути структуровані таким чином:

1. **Надійність системи (Reliability).** Відповідні стандарти: IEEE 1451, ITU-T Y.2060, ISO/IEC 25010:

- 1.1. Відсоток безвідмовної роботи за визначений період часу ($\text{Availability} \geq 99.9\%$) [21].
- 1.2. Середній час між відмовами (MTBF - Mean Time Between Failures).
- 1.3. Виявлення та обробка збоїв [15].
- 1.4. Механізми виявлення та відновлення після збоїв (redundancy, failover) [16].

2. **Продуктивність передачі даних (Performance Metrics).** Відповідні стандарти: IETF RFC 8200 (IPv6), RFC 7252 (CoAP), RFC 8446 (TLS 1.3), ITU-T Y.4000, IEEE 802.15.4:

- 2.1 Пропускна здатність (Throughput) [18] - Вимірюється в біт/с; залежить від використаних протоколів (наприклад, MQTT, CoAP, Zigbee).
- 2.2 Затримка (Latency) - Час передачі даних від датчика до обробника [19].
- 2.3 Джитер (Jitter) - Варіативність затримок між пакетами.
- 2.4 Доступність (Availability) – Відсоток часу, коли система перебуває в робочому стані, наприклад, $> 99,9\%$ [21].

3. **Масштабованість (Scalability).** Відповідні стандарти: ITU-T Y.2060, IEEE P2413, IETF RFC 6924:

- 3.1 Підтримка великої кількості одночасно підключених пристроїв (від 10 до 10 000+) [16].
- 3.2 Підтримка зростання без зміни архітектури [19].
- 3.3 Інтєрооперабельність через стандартизовані протоколи MQTT, CoAP [17; 18].

4. **Енергоспоживання (Energy Efficiency).** Відповідні стандарти: IEEE 802.15.4, IEEE 802.11ah (Wi-Fi HaLow), ETSI EN 303 204:

- 4.1 Рівень енергоспоживання на одиницю обробки інформації [14].
- 4.2 Споживання енергії в активному режимі та у стані очікування [4].
- 4.3 Енергоефективні мережі — LoRa, Zigbee, 802.15.4e [14; 16].

5. **Безпека та конфіденційність (Security and Privacy).** Відповідні стандарти: ISO/IEC 27001, ISO/IEC 29100, IETF RFC 6280, RFC 8576 (IoT Security Considerations):

- 5.1 Захист каналів зв'язку (TLS, DTLS) [17; 22];
- 5.2 Аутентифікація пристроїв — CBOR Web Token (RFC 8392) [25].
- 5.3 Криптографія для обмежених пристроїв (ECC, DSA) [23].
- 5.4 Захист персональних даних (GDPR/ISO 27701) [22].

6. **Точність та достовірність даних (Accuracy and Data Quality).** Відповідні стандарти: IEEE 1451.5, ISO/IEC 25012 (Data Quality Model):

- 6.1 Калібрування сенсорів [24];
- 6.2 Верифікація та фільтрація даних (noise filtering) [15];
- 6.3 Нормалізація сигналів [15].

7. Адаптивність та гнучкість системи (Flexibility). Відповідні стандарти: IEEE P2413, ITU-T Y.3011 :

7.1 Можливість динамічного оновлення прошивки (OTA).

7.2 Інтероперабельність: підтримка різних протоколів (MQTT, CoAP, LwM2M) [17, 18].

7.3 Придатність до модифікацій без повної реконфігурації мережі [15; 26].

Що стосується систем типу «розумний дім», то тут є свої особливості, які мають бути враховані. Так, компанії Philips Hue, Google Nest, Amazon Alexa, Xiaomi Smart Home часто вказують вимоги до швидкості реакції системи — менш як 100 мс, особливо для інтерактивного керування [17]. Люди сприймають затримку понад ~100 мс як "відчутну". Якщо світло не загоряється миттєво після клацання або команди, це сприймається як помилка. Безпека — ще критичніша: сигнал тривоги або блокування дверей має відбутись негайно. Тож, для таких систем доцільно розширити розгляд низки важливих показників, які у попередньому викладі були окреслені лише на рівні загального переліку. Зокрема, йдеться про такі аспекти, як енергоспоживання, безпека та конфіденційність, а також точність і достовірність даних.

Енергоспоживання є ключовим показником IoT-систем, особливо тих, що працюють від автономних джерел живлення (батарей або акумуляторів). Вона визначає тривалість безперервної роботи пристроїв та впливає на загальну експлуатаційну вартість системи. За стандартами IEEE 802.15.4, IEEE 802.11ah та ETSI EN 303 204, важливо оцінювати не лише абсолютне споживання енергії в активному та пасивному режимах, а й ефективність енергоспоживання на одиницю переданих або оброблених даних [14; 16].

Типові значення енергоспоживання для сенсорних пристроїв у системах «розумного дому» не повинні перевищувати 100 мВт·год, що дозволяє забезпечити багаторічний термін роботи без заміни джерел живлення. Використання енергоефективних протоколів (LoRa, Zigbee, IEEE 802.15.4e) сприяє зниженню енергоспоживання, одночасно підтримуючи необхідний рівень продуктивності [14].

Недостатня енергоефективність призводить до частих замін батарей, підвищення експлуатаційних витрат і ризику перебоїв у роботі системи, що знижує її загальну ефективність.

Безпека та конфіденційність є критично важливими для забезпечення надійної роботи IoT-систем та захисту даних користувачів. Відсутність належних механізмів безпеки може призвести до несанкціонованого доступу, втрати або спотворення даних, а також до втрати контролю над пристроями [17; 22].

Основні стандарти ISO/IEC 27001, ISO/IEC 29100 та RFC 6280 регламентують вимоги до захисту каналів зв'язку (TLS, DTLS), аутентифікації пристроїв (CBOR Web Token) та криптографії (ECC, DSA) для ресурсно обмежених пристроїв [23; 25]. Захист персональних даних, зокрема у відповідності до GDPR/ISO 27701, підвищує довіру користувачів і є законодавчою вимогою в багатьох країнах.

Типові рівні шифрування, що застосовуються в IoT, включають AES-128, TLS, WPA2, які забезпечують достатній рівень безпеки для більшості застосувань. Важливість безпеки оцінюється як критична, оскільки її порушення може призвести до серйозних фінансових та репутаційних втрат.

Точність та достовірність даних є важливими для забезпечення коректності рішень, прийнятих на основі IoT-систем. Відхилення або шум у зібраних даних можуть призвести до помилкових висновків та зниження ефективності системи [15; 24].

Стандарти IEEE 1451.5 та ISO/IEC 25012 визначають методи калібрування сенсорів, верифікації та фільтрації даних (noise filtering), а також нормалізації сигналів, що дозволяють підвищити якість інформації. Типові вимоги передбачають похибку не більше як 5 %, що є достатнім для більшості прикладних сценаріїв у «розумному домі». Висока точність даних підвищує довіру до системи та дозволяє більш ефективно використовувати отриману інформацію для автоматизації і прийняття рішень.

На основі узагальнення стандартів, типових технічних метрик та критичності застосування, пропонується базова структурована модель оцінювання ефективності IoT-систем, представлена у вигляді табл. 1.

Таблиця 1 – Базова структурована модель оцінювання ефективності IoT-систем

Властивості	Показники (метрики)	Одиниця виміру	Типові значення	Важливість
Надійність	Безвідмовність, середній час між відмовами, виявлення/обробка збоїв	% або MTBF (годин)	> 99,9% або > 10 000 год	Висока
Продуктивність передачі	Пропускна здатність, затримка, джитер, доступність	Кбіт/с, мс, %	100 Кбіт/с – 10 Мбіт/с; <100 мс; >99.9%	Критична для систем реального часу
Масштабованість	Кількість підключених пристроїв, сумісність протоколів	Кількість пристроїв	> 10 000 пристроїв	Висока
Енергоспоживання	Потужність у режимі очікування/активному, енергоефективні технології	мВт, Вт·год	< 100 мВт/год (для сенсорів)	Важлива для IoT-батарей
Безпека та конфіденційність	Шифрування, автентифікація, захист персональних даних	Якісна оцінка / тип криптографії	TLS, DTLS, AES-128, ECC	Критично важлива
Точність та достовірність	Калібрування, фільтрація шуму, нормалізація	% похибки	< 5%	Висока
Адаптивність та гнучкість	ОТА-оновлення, підтримка протоколів, гнучкість конфігурації	Кількість змін / підтримка ОТА	До 5 змін без перебудови, ОТА доступне	Висока

Ця модель включає сім ключових груп показників, кожна з яких характеризує окрему функціональну складову системи, і може слугувати основою для перспективного оцінювання відповідності IoT-системи цільовим критеріям у прикладних доменах.

Для кращого розуміння практичного застосування техніко-експлуатаційних показників ефективності функціонування IoT-систем у контексті «розумного дому», нижче наведено приклад (табл. 2) конкретних граничних значень та відповідних стандартів, що регламентують ці показники. Ці критерії дозволяють забезпечити оцінити стабільність, масштабованість та енергоефективність систем, які функціонують у реальному часі.

Таблиця 2 – Приклад застосування моделі оцінки IoT-системи «Розумний дім»

Показник	Типове значення	Результат системи	Оцінка
Затримка	< 100 мс	140мс	-
Надійність	> 99.9%	99.95%	+
Продуктивність передачі	100 Кбіт/с – 10 Мбіт/с	1.5 Мбіт/с	+
Енергоспоживання сенсорів	< 100 мВт·год	120 мВт·год	-
Безпека	Відповідає стандартам	TLS+ECC+CBOR Token	+
Точність	< 5%	±3%	+
Адаптивність	Мінімум 2, ОТА підтримка	ОТА доступне, 3 протоколи	+

Таким чином, система відповідає 5 із 7 критичних показників. Затримка перевищує межі реального часу, а енергоспоживання сенсорів вимагає оптимізації. Результат може бути поданий як карта відповідності, що слугує вхідними даними для прийняття рішень щодо модернізації або масштабування.

Для практичного використання запропонованої вище моделі перспективного оцінювання ефективності IoT-систем, у тому числі із застосуванням когнітивних карт, пропонується такий алгоритм:

1. **Ідентифікація системи.** Визначити межі аналізу: тип IoT-системи, кількість пристроїв, сферу застосування (eHealth, Smart Home, IIoT тощо).

2. **Отримання вихідних технічних характеристик.** Перевірити шляхом математичного моделювання фактичні значення основних метрик (надійність, продуктивність передачі, енергоспоживання, безпека, точність, адаптивність тощо).

3. **Зіставлення з критеріями моделі.** Порівняти отримані показники з типовими/еталонними значеннями із табл. 2.

4. **Оцінка відповідності.** Для кожної метрики визначити: відповідає / не відповідає (наприклад, кольором або балами).

5. **Візуалізація відповідності.** Побудувати діаграму (наприклад, radar chart або матрицю відповідності) для візуального аналізу.

6. **Формування висновку.** На основі кількості відповідностей (наприклад, ≥ 5 із 7 – прийнятна ефективність) зробити висновок про доцільність використання, масштабування або вдосконалення системи.

7. **Рекомендації.** Визначити метрики, які потребують покращення, та можливі заходи (заміна сенсорів, оптимізація протоколу, перехід на edge-обчислення тощо).

Висновки. У роботі представлено систематизований підхід до оцінювання ефективності IoT-систем з урахуванням ключових техніко-експлуатаційних показників: надійності, затримки, пропускну здатності, масштабованості, енергоспоживання, безпеки, точності та гнучкості. Для кожного з параметрів визначено типові значення, релевантні одиниці виміру, критичні значення та відповідні міжнародні стандарти (наприклад, ISO/IEC 25010, ITU-T Y.2060, IEEE 802.15.4, IEEE P2413).

Особливу увагу приділено системам реального часу на прикладі «розумного дому», де ефективність значною мірою залежить від дотримання мінімальних затримок, високої надійності та здатності до динамічної адаптації.

Також проаналізовано сучасні підходи до перспективного оцінювання, які доповнюють класичні метрики когнітивними критеріями, формалізованими моделями, показниками досвіду користувача (UX) та міжплатформенною сумісністю. Такий підхід дозволяє здійснювати більш точне планування розвитку IoT-систем та оцінювати їхню ефективність за різними сценаріями функціонування.

Крім того, у роботі запропоновано базову структуровану модель оцінювання ефективності IoT-систем та методичний алгоритм її практичного використання. Запропоновані приклади демонструють можливість формалізованого порівняння фактичних характеристик системи з нормативними показниками, що створює підґрунтя для прийняття рішень щодо оптимізації або масштабування архітектури. Такий підхід підвищує об'єктивність технічного аудиту та сприяє підготовці адаптивних стратегій розвитку IoT-рішень у різних предметних галузях. Описана модель оцінювання може бути розширена з урахуванням специфіки конкретних галузей (наприклад, промисловість, агросектор, охорона здоров'я) і використовуватися як частина інструментарію проєктування, аудиту або вдосконалення IoT-систем.

Список використаних джерел

1. Usik, A., & Kazymyr, V. (2019). Evaluation cognitive maps for extended technology roadmapping in iot. In *2019 10th IEEE international conference on intelligent data acquisition and advanced computing systems: Technology and applications (IDAACS)*. IEEE. <https://doi.org/10.1109/idaacs.2019.8924442>
2. Klima, M., Hanzálek, I., & Švéda, P. (n.d.). *Quality and reliability metrics for IoT systems: A consolidated view*. Abertay Research Portal. <https://rke.abertay.ac.uk>

3. Martinsson Bonde, J., Kokkolaras, M., Andersson, P., Panarotto, M., & Isaksson, O. (2023). A similarity-assisted multi-fidelity approach to conceptual design space exploration. *Computers in Industry*, 151, 103957. <https://doi.org/10.1016/j.compind.2023.103957>.
4. Ray, P. P., & Chatterjee, S. (2020). *IoT reliability: A review leading to 5 key research directions*. ResearchGate.
5. El-Dosuky, M., El-Bakry, H., & Bahgat, A. (2023). Enhancing IoT performance in wireless and mobile networks. *Simulation Modelling Practice and Theory*. <https://doi.org/10.1016/j.simpat.2023.102755>.
6. Villalba, L. J., Naranjo, P. A., & Casilari, E. (2020). Quality characteristics in IoT systems: Learnings from an industry survey and workshop. *Software Quality Journal*.
7. Al-Turjman, F., Mostarda, L., & Giudice, G. D. (2020). *IoT reliability: A review leading to 5 key research directions*. ResearchGate. https://www.researchgate.net/publication/343512706_IoT_reliability_a_review_leading_to_5_key_research_directions.
8. Shukla, P. K., Jaiswal, A., Sharma, A., & Park, J. H. (2020). *A systematic review on performance evaluation metric selection for various IoT applications*. arXiv. <https://arxiv.org/abs/2007.12238>.
9. Moulla, D. K., Mnkandla, E., & Abran, A. (2023). Evaluation of IoT measurement solutions from a metrology perspective. *Computer Systems Science and Engineering*, 47(2), 2455–2479. <https://doi.org/10.32604/csse.2023.039736>.
10. Han, R., Huang, R., & Wang, Y. (2024). Performance evaluation in an IoT-based ecosystem — A field study approach. *SSRN*. <https://doi.org/10.2139/ssrn.4967215>.
11. Almalki, A., & Mourshed, M. (2024). Occupant-centric key performance indicators for intelligent buildings: A systematic review. *Building and Environment*, 246, 111435. <https://doi.org/10.1016/j.buildenv.2024.111435>.
12. Luo, Y., & Yu, S. (2023). Industrial Internet of Things: Standardization, challenges and future directions. *Future Generation Computer Systems*, 141, 165–182. <https://doi.org/10.1016/j.future.2023.03.006>.
13. Villalba, L. J., Naranjo, P. A., & Casilari, E. (2020). Quality characteristics in IoT systems: Learnings from an industry survey and workshop. *SpringerLink*. <https://link.springer.com>.
14. IEEE. (2020). *IEEE 802.15.4: IEEE standard for low-rate wireless networks*. https://standards.ieee.org/standard/802_15_4-2020.html
15. IEEE. (2019). *IEEE 2413-2019: IEEE standard for an architectural framework for the Internet of Things*. <https://standards.ieee.org/standard/2413-2019.html>.
16. International Organization for Standardization. (2018). *ISO/IEC 30141:2018 – Інтернет речей (IoT): Референтна архітектура*.
17. Shelby, Z., Hartke, K., & Bormann, C. (2014). *The constrained application protocol (CoAP) (RFC 7252)*. Internet Engineering Task Force (IETF). <https://datatracker.ietf.org/doc/html/rfc7252>.
18. Hunkeler, U., Truong, H. L., & Stanford-Clark, A. (2020). *MQTT version 5.0 (RFC 8967)*. Internet Engineering Task Force (IETF). <https://datatracker.ietf.org/doc/html/rfc8967>.
19. International Telecommunication Union. (2012). *ITU-T Y.2060: Overview of the Internet of Things*. <https://www.itu.int/rec/T-REC-Y.2060-201206-I/en>.
20. International Telecommunication Union. (2019). *ITU-T Y.4208: Requirements and capabilities for interworking of IoT*. <https://www.itu.int/rec/T-REC-Y.4208-201908-I/en>.
21. International Organization for Standardization & International Electrotechnical Commission. (2011). *ISO/IEC 25010:2011 – Системна та програмна інженерія: Якісні вимоги та оцінювання (SQuaRE)*.
22. International Organization for Standardization & International Electrotechnical Commission. (2019). *ISO/IEC 27701:2019 – Розширення до ISO/IEC 27001 та ISO/IEC 27002 для управління конфіденційною інформацією*.
23. International Organization for Standardization & International Electrotechnical Commission. (n.d.). *ISO/IEC 29192 – Легковагова криптографія*.
24. International Organization for Standardization & International Electrotechnical Commission. (2017). *ISO/IEC 17025:2017 – Загальні вимоги до компетентності випробувальних та калібрувальних лабораторій*.
25. Jones, M., & Wahlstroem, H. (2018). *CBOR Web Token (CWT) (RFC 8392)*. Internet Engineering Task Force (IETF). <https://datatracker.ietf.org/doc/html/rfc8392>.

26. International Telecommunication Union. (2012). *ITU-T Y.3011: Framework of networked vehicle platforms based on cloud computing*. <https://www.itu.int/rec/T-REC-Y.3011-201212-I/en>.

References

1. Usik, A., & Kazymyr, V. (2019). Evaluation cognitive maps for extended technology roadmapping in iot. In *2019 10th IEEE international conference on intelligent data acquisition and advanced computing systems: Technology and applications (IDAACS)*. IEEE. <https://doi.org/10.1109/idaacs.2019.8924442>.
2. Klima, M., Hanzálek, I., & Švéda, P. (n.d.). *Quality and reliability metrics for IoT systems: A consolidated view*. Abertay Research Portal. <https://rke.abertay.ac.uk>.
3. Martinsson Bonde, J., Kokkolaras, M., Andersson, P., Panarotto, M., & Isaksson, O. (2023). A similarity-assisted multi-fidelity approach to conceptual design space exploration. *Computers in Industry*, 151, 103957. <https://doi.org/10.1016/j.compind.2023.103957>.
4. Ray, P. P., & Chatterjee, S. (2020). *IoT reliability: A review leading to 5 key research directions*. ResearchGate.
5. El-Dosuky, M., El-Bakry, H., & Bahgat, A. (2023). Enhancing IoT performance in wireless and mobile networks. *Simulation Modelling Practice and Theory*. <https://doi.org/10.1016/j.simpat.2023.102755>.
6. Villalba, L. J., Naranjo, P. A., & Casilari, E. (2020). Quality characteristics in IoT systems: Learnings from an industry survey and workshop. *Software Quality Journal*.
7. Al-Turjman, F., Mostarda, L., & Giudice, G. D. (2020). *IoT reliability: A review leading to 5 key research directions*. ResearchGate. https://www.researchgate.net/publication/343512706_IoT_reliability_a_review_leading_to_5_key_research_directions.
8. Shukla, P. K., Jaiswal, A., Sharma, A., & Park, J. H. (2020). *A systematic review on performance evaluation metric selection for various IoT applications*. arXiv. <https://arxiv.org/abs/2007.12238>.
9. Moulla, D. K., Mnkandla, E., & Abran, A. (2023). Evaluation of IoT measurement solutions from a metrology perspective. *Computer Systems Science and Engineering*, 47(2), 2455–2479. <https://doi.org/10.32604/csse.2023.039736>.
10. Han, R., Huang, R., & Wang, Y. (2024). Performance evaluation in an IoT-based ecosystem — A field study approach. *SSRN*. <https://doi.org/10.2139/ssrn.4967215>.
11. Almalki, A., & Mourshed, M. (2024). Occupant-centric key performance indicators for intelligent buildings: A systematic review. *Building and Environment*, 246, 111435. <https://doi.org/10.1016/j.buildenv.2024.111435>.
12. Luo, Y., & Yu, S. (2023). Industrial Internet of Things: Standardization, challenges and future directions. *Future Generation Computer Systems*, 141, 165–182. <https://doi.org/10.1016/j.future.2023.03.006>.
13. Villalba, L. J., Naranjo, P. A., & Casilari, E. (2020). Quality characteristics in IoT systems: Learnings from an industry survey and workshop. *SpringerLink*. <https://link.springer.com>.
14. IEEE. (2020). *IEEE 802.15.4: IEEE standard for low-rate wireless networks*. https://standards.ieee.org/standard/802_15_4-2020.html
15. IEEE. (2019). *IEEE 2413-2019: IEEE standard for an architectural framework for the Internet of Things*. <https://standards.ieee.org/standard/2413-2019.html>.
16. International Organization for Standardization. (2018). *ISO/IEC 30141:2018 – nternet of Things (IoT) – Reference architecture*.
17. Shelby, Z., Hartke, K., & Bormann, C. (2014). *The constrained application protocol (CoAP) (RFC 7252)*. Internet Engineering Task Force (IETF). <https://datatracker.ietf.org/doc/html/rfc7252>.
18. Hunkeler, U., Truong, H. L., & Stanford-Clark, A. (2020). *MQTT version 5.0 (RFC 8967)*. Internet Engineering Task Force (IETF). <https://datatracker.ietf.org/doc/html/rfc8967>.
19. International Telecommunication Union. (2012). *ITU-T Y.2060: Overview of the Internet of Things*. <https://www.itu.int/rec/T-REC-Y.2060-201206-I/en>.
20. International Telecommunication Union. (2019). *ITU-T Y.4208: Requirements and capabilities for interworking of IoT*. <https://www.itu.int/rec/T-REC-Y.4208-201908-I/en>.
21. International Organization for Standardization & International Electrotechnical Commission. (2011). *ISO/IEC 25010:2011 – Systems and Software Engineering: Quality Requirements and Evaluation (SQuaRE)*.

22. International Organization for Standardization & International Electrotechnical Commission. (2019). *ISO/IEC 27701:2019 – Extension to ISO/IEC 27001 and ISO/IEC 27002 for the management of confidential information*.

23. International Organization for Standardization & International Electrotechnical Commission. (n.d.). *ISO/IEC 29192 – Lightweight cryptography*.

24. International Organization for Standardization & International Electrotechnical Commission. (2017). *ISO/IEC 17025:2017 – General requirements for the competence of testing and calibration laboratories*.

25. Jones, M., & Wahlstroem, H. (2018). *CBOR Web Token (CWT) (RFC 8392)*. Internet Engineering Task Force (IETF). <https://datatracker.ietf.org/doc/html/rfc8392>.

26. International Telecommunication Union. (2012). *ITU-T Y.3011: Framework of networked vehicle platforms based on cloud computing*. <https://www.itu.int/rec/T-REC-Y.3011-201212-I/en>.

Отримано 11.06.2025

UDC 37:004.738

Anna Usik¹, Volodymyr Kazymyr²

¹Assistant of the Department of Information and Computer Systems
Chernihiv Polytechnic National University (Chernihiv, Ukraine)

E-mail: usik18@gmail.com. **ORCID:** <https://orcid.org/0000-0003-4965-6863>. **ResearcherID:** E-2911-2019

²Doctor of Technical Sciences, Professor of the Department of Information and Computer Systems
Chernihiv Polytechnic National University (Chernihiv, Ukraine)

E-mail: vykazymyr@gmail.com. **ORCID:** <https://orcid.org/0000-0001-8163-1119>. **ResearcherID:** Q-2925-2016

PERFORMANCE INDICATORS FOR PROSPECTIVE EVALUATION OF INTERNET OF THINGS SYSTEMS

Rapid development and integration of the Internet of Things (IoT) into various domains of human activity underscores the growing importance of evaluating the operational efficiency of such systems. Modern smart environments, industrial automation platforms, and intelligent infrastructures rely heavily on networks of interconnected devices and sensors that generate, exchange, and process large volumes of data. Given the wide applicability of IoT and the continuous growth in the number of connected devices, ensuring their efficiency and reliability becomes critically important. The relevance of this research is driven by the need to define comprehensive, technically grounded, and practically applicable performance indicators that can guide the design, deployment, and optimization of IoT systems.

This study addresses the problem of identifying, systematizing, and structuring key performance indicators for IoT systems to ensure their suitability for specific use cases. Current challenges include balancing throughput, energy efficiency, latency, scalability, reliability, and data accuracy. Without a structured evaluation framework, it becomes difficult to ensure that IoT systems comply with functional and quality-of-service requirements, particularly in critical domains such as healthcare, infrastructure, and smart homes.

The aim of this research is to formalize and generalize the key technical and operational metrics that determine the efficiency of IoT systems. These include reliability, latency, energy consumption, scalability, security, and data quality. A structured model of performance evaluation is proposed, incorporating typical threshold values, measurement units, and relevant international standards. Additionally, the study emphasizes the use of formalized modeling tools—such as cognitive maps and E-net models—for enhanced analysis and decision-making in distributed IoT environments.

The methodology combines the analysis of international standards, scientific literature, and practical implementations in real-world scenarios. A structured classification of performance indicators is presented, supported by a practical example of a smart home system. Moreover, a methodical algorithm is proposed for the systematic assessment of IoT performance, allowing stakeholders to compare actual system characteristics against standard benchmarks.

The results of this study show that the most impactful indicators for IoT efficiency include reliability, latency, energy consumption, and data accuracy. These metrics significantly influence system responsiveness, service continuity, and data integrity. The proposed model and algorithm can be used as a methodological basis for technical audits, scenario-based planning, and the development of adaptive and scalable IoT ecosystems. The findings contribute to both the scientific understanding and the practical evaluation of efficiency in IoT systems and may serve as a foundation for future research and development in this field.

Keywords: Internet of Things; efficiency; technical and operational indicators; smart home; reliability; responsiveness; energy consumption; prospective evaluation.

Table: 2. References: 26.