

DOI: <https://doi.org/10.36910/6775-2524-0560-2025-60-23>

УДК 004.415:004.738.5

Мусієнко Максим Павлович¹, д.т.н., професор

<https://orcid.org/0000-0001-9228-2233>

Мусієнко Олена Юріївна², здобувач

¹ Черкаський національний університет ім. Б.Хмельницького, м. Черкаси, Україна

² Чорноморський національний університет ім. П.Могили, м. Миколаїв, Україна

ІНТЕГРАЦІЯ ІОТ-СИСТЕМ ЗБОРУ СЕНСОРНИХ ДАНИХ НА ОСНОВІ П'ЄЗОКЕРАМІЧНИХ ДАТЧИКІВ У ХМАРНУ ІНФРАСТРУКТУРУ AWS

Мусієнко М. П., Мусієнко О. Ю. Інтеграція ІоТ-систем збору сенсорних даних на основі п'єзокерамічних датчиків у хмарну інфраструктуру AWS. У статті розглядаються методи та засоби інтеграції ІоТ-систем збору сенсорних даних, що базуються на п'єзокерамічних датчиках, у хмарну інфраструктуру Amazon Web Services (AWS). Представлено архітектурну модель побудови ІоТ-системи з урахуванням вибору протоколів зв'язку, типових інтерфейсів, форматів передачі та сервісів AWS (IoT Core, Lambda, Timestream, DynamoDB, S3, CloudWatch). Проведено порівняльний аналіз можливостей застосування протоколів передачі даних у контексті обмежених обчислювальних ресурсів та специфіки сигналів від п'єзодатчиків. Особливу увагу приділено питанням безпечної автентифікації пристроїв за допомогою X.509-сертифікатів, а також захисту даних при передачі. Запропоновано підхід до побудови відмовостійкої хмарної архітектури із застосуванням доступних зон AWS. Описано приклад експериментальної реалізації на основі ESP32 та п'єзоелементів muRata з передачею даних до хмари та збереженням у Timestream. Результати досліджень демонструють ефективність інтегрованої системи для завдань моніторингу вібрацій та перспективність застосування таких рішень у промислових та інженерних задачах.

Ключові слова: ІоТ, п'єзокерамічні датчики, AWS, хмарна інтеграція, AWS IoT Core, AWS Lambda.

Musiienko M., Musiienko O. Integration of Sensor Data Collection IoT Systems Based on Piezoceramic Sensors into the AWS Cloud Infrastructure. The article explores the methods and tools for integrating IoT systems for sensor data collection based on piezoelectric ceramic sensors into the Amazon Web Services (AWS) cloud infrastructure. An architectural model of the IoT system is presented, taking into account the choice of communication protocols, standard interfaces, data transmission formats, and AWS services (IoT Core, Lambda, Timestream, DynamoDB, S3, CloudWatch). A comparative analysis is conducted on the applicability of various data transmission protocols in the context of limited computational resources and the specific characteristics of piezoelectric sensor signals. Special attention is given to the secure authentication of devices using X.509 certificates, as well as to the protection of data during transmission. A resilient cloud architecture approach is proposed using AWS availability zones. An example of an experimental implementation is described based on the ESP32 platform and muRata piezo elements, with data transmitted to the cloud and stored in Timestream. The research results demonstrate the effectiveness of the integrated system for vibration monitoring tasks and highlight the potential of such solutions in industrial and engineering applications.

Keywords: IoT, piezoceramic sensors, AWS, cloud integration, AWS IoT Core, AWS Lambda.

Постановка наукової проблеми. Сучасні тенденції в розвитку Інтернету речей (Internet of Things, IoT) зумовлюють зростання потреби у створенні систем збору, передачі та обробки сенсорних даних у реальному часі. Особливої актуальності набувають ІоТ-рішення, які базуються на високочутливих сенсорах, зокрема п'єзокерамічних датчиках, здатних фіксувати тиск, вібрації, деформації та інші фізичні величини. Висока чутливість таких сенсорів відкриває нові можливості для моніторингу об'єктів, структур та технологічних процесів у промисловості, енергетиці, транспорті та інженерії.

Однак ефективне використання даних, що надходять від п'єзокерамічних ІоТ-датчиків, потребує їхньої обробки, зберігання та аналізу у масштабованому та надійному середовищі. З цією метою дедалі частіше використовуються хмарні обчислювальні платформи, зокрема Amazon Web Services (AWS), які надають широкий набір інструментів для підключення, керування та обробки даних з ІоТ-пристроїв. Разом з тим, процес інтеграції таких сенсорних ІоТ-систем із хмарними сервісами не є тривіальним і пов'язаний із низкою наукових та інженерних проблем та задач. До таких задач належать:

- забезпечення безвідмовного функціонування пристрою при обмежених обчислювальних та енергетичних ресурсах на стороні ІоТ-пристрою;
- вибір відповідного протоколу передачі даних (наприклад, MQTT, HTTPS);
- реалізація безпечного каналу передачі даних від ІоТ-датчиків до хмари;
- побудова ефективної та надійної архітектури взаємодії між ІоТ-пристроями і хмарними сервісами (AWS IoT Core, AWS Lambda, Amazon DynamoDB тощо);

Наукова проблема полягає у розробці методів та засобів ефективної, масштабованої та безпечної інтеграції п'єзокерамічних ІоТ-сенсорів із хмарною інфраструктурою AWS з

урахуванням особливостей генерації та передачі сигналів, обмежених енергетичних ресурсів IoT-вузлів, необхідності обробки великих потоків даних, а також вимог до надійності та швидкодії. Практичне значення вирішення цієї проблеми полягає у створенні універсальних архітектур та рішень, які можуть бути задіяні для різних задач моніторингу та діагностики.

Таким чином, актуальність теми дослідження обумовлена одночасно зростанням потреб у використанні високочутливих п'єзокерамічних датчиків для моніторингу об'єктів та технологічних процесів, а також необхідністю забезпечення їх надійної та ефективної інтеграції у хмарні середовища обробки даних. Розв'язання поставленої проблеми дозволить підвищити ефективність функціонування IoT-систем на основі п'єзокерамічних датчиків та сприятиме подальшому розвитку інтелектуальних кіберфізичних систем у різних сферах господарства.

Аналіз останніх досліджень. Сучасні дослідження в галузі інтеграції IoT-систем із хмарними сервісами показують різноманітні підходи до вирішення технічних та архітектурних завдань. Наприклад, в роботі [1] показано використання AWS IoT Core для створення системи детекції руху, де Edge-пристрої синхронізуються з Lambda-функціями для обробки відеоданих, що демонструє важливість подієвої архітектури для обробки даних у реальному часі.

В роботі [2] при дослідженні питання масштабованого зберігання сенсорних даних запропоновано концепцію Sensor-Cloud, яка інтегрує WSN із хмарними сховищами через спеціалізовані шлюзи. Цей підхід оптимізує передачу стиснених даних із подальшою декомпресією на стороні хмари, що особливо актуально для п'єзокерамічних сенсорів з високою частотою вибірок.

Архітектурні рішення для IoT-хмарної інтеграції детально описані в офіційній документації AWS [3], де запропоновано трирівневу модель: збір даних через IoT Core, їхнє зберігання в DocumentDB та аналіз за допомогою машинного навчання. Для часових рядів від датчиків рекомендується використання Amazon Timestream [4], що підтверджується прикладами із моніторингу промислового обладнання.

Важливим питанням є безпека передачі даних, яка досліджена багатьма авторами. Зокрема, як приклад, в дослідженні [2] пропонують механізми двофакторної автентифікації через AWS Cognito, що запобігає несанкціонованому доступу до сенсорних мереж. Практична реалізація захищених з'єднань детально описана в керівництві AWS IoT Core [5], де акцентовано увагу на використанні X.509 сертифікатів.

Для обробки великих потоків даних в роботі [6] для отримання даних використано архітектуру з Kinesis, для трансформації - AWS Lambda та для аналітики - Amazon Redshift, що підтверджує ефективність serverless підходу для динамічних IoT-навантажень.

Проте при наявності значної кількості досліджень побудови IoT-систем та їхньої інтеграції з хмарними обчислювальними платформами, більшість існуючих рішень зосереджуються на універсальних або загальних сенсорних модулях і не враховують специфіку роботи п'єзокерамічних датчиків. У той час як у ряді публікацій розглядаються питання вибору протоколів обміну даними, маршрутизації та обробки інформації в хмарному середовищі, практично відсутні дослідження, що комплексно аналізують технічні й архітектурні виклики, які виникають саме при підключенні п'єзокерамічних сенсорів до хмарної інфраструктури AWS.

Таким чином, дана робота присвячена розгляду менш дослідженої частини зазначеної проблеми - інтеграції сенсорних IoT-систем на базі п'єзокерамічних датчиків у хмарну інфраструктуру AWS з урахуванням їхніх фізичних та функціональних особливостей, а також вимог до обробки та візуалізації отриманих даних у хмарному середовищі.

Мета роботи полягає у розробці методів і засобів інтеграції IoT-систем збору сенсорних даних на основі п'єзокерамічних датчиків у хмарну інфраструктуру AWS з урахуванням особливостей архітектури хмарних сервісів, вибору оптимальних протоколів передачі, забезпечення надійної та безпечної взаємодії між пристроями та хмарою, а також з можливістю масштабування, обробки і подальшого аналізу отриманих даних у режимі реального часу.

Виклад основного матеріалу дослідження. Для забезпечення ефективної інтеграції IoT-систем збору сенсорних даних на основі п'єзокерамічних датчиків у хмарну інфраструктуру AWS необхідно враховувати комплекс інженерних, архітектурних та програмно-мережевих питань.

На основі попереднього аналізу проблеми було визначено основні компоненти IoT-архітектури, які слід врахувати при побудові системи збору даних з п'єзокерамічних сенсорів та їх інтеграції з сервісами Amazon Web Services.

Структурну схему IoT-системи збору сенсорних даних на основі п'єзокерамічних датчиків із передачею до хмар AWS наведено на рис. 1, де показана загальна структура, починаючи від збору даних сенсорами і завершуючи візуалізацією та аналітикою в хмарі.

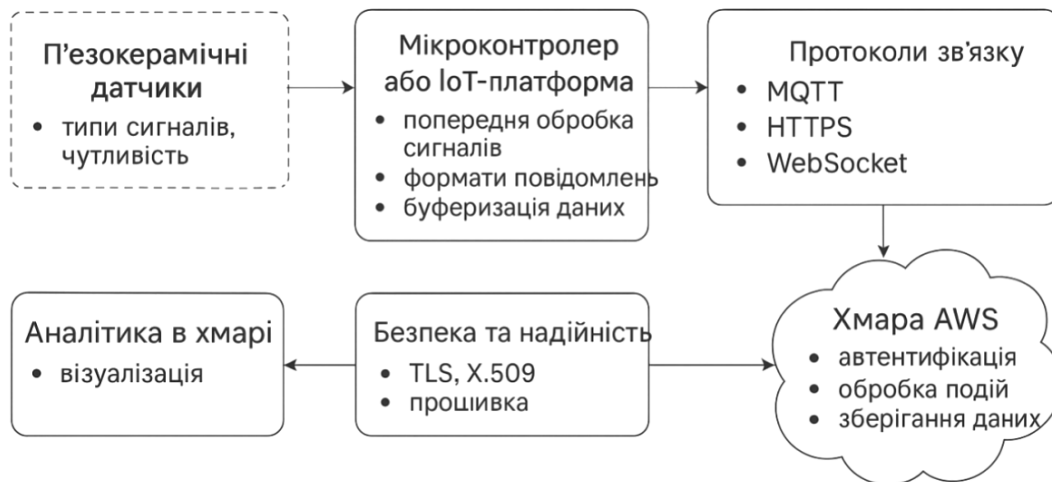


Рис. 1. Структурна схема IoT-системи збору сенсорних даних на основі п'єзокерамічних датчиків із передачею до хмар AWS

Ключовими питаннями побудови такої системи, є технічні особливості сенсорів, вибір мікроконтролера, формування повідомлень, вибір протоколів передачі, безпека передавання даних, використання AWS IoT Core та суміжних сервісів для обробки подій, зберігання інформації та реалізація аналізу даних. Всі ці питання можна згрупувати у 6 напрямів:

- архітектура IoT-системи з п'єзокерамічними датчиками;
- формування та передача даних із пристрою;
- вибір протоколів зв'язку для інтеграції з хмарою AWS;
- інтеграція з хмарною інфраструктурою AWS;
- аналітика, візуалізація та обробка даних у хмарі AWS;
- забезпечення безпеки та надійності системи.

Архітектура IoT-системи з п'єзокерамічними датчиками. Питання побудови IoT-систем на основі п'єзокерамічних сенсорів уже тривалий час досліджуються в науковій літературі та на практиці, і на сьогодні сформовано низку рекомендацій щодо вибору елементної бази, способів зчитування сигналів та попередньої обробки даних. В якості IoT-платформи найчастіше застосовують ESP32, STM32 або Raspberry Pi - залежно від вимог до обчислювальних ресурсів, енергоспоживання та засобів зв'язку. Для оцифрування сигналів використовують вбудовані або зовнішні аналого-цифрові перетворювачі, що з'єднані через інтерфейси типу SPI або I²C.

До питань, які при цьому вирішуються, слід віднести підвищений рівень шумів, необхідність у стабільному живленні, захист від завадних сигналів, а також забезпечення надійного формування повідомлень для подальшої передачі у хмару. Саме тому попереднє формування пакетів сенсорних даних та коректна обробка первинних даних датчика є критично важливим етапом перед передачею інформації до хмарних сервісів AWS.

Проте дана стаття зосереджується, насамперед, на інтеграції сенсорних IoT-систем до хмарної інфраструктури AWS, тому детально розглядати питання архітектури IoT-системи з п'єзокерамічними датчиками не має сенсу.

Те ж саме стосується й другого важливого питання: *формування та передача даних із пристрою*, що є одним з ключових етапів інтеграції IoT-системи з хмарною інфраструктурою, тобто попереднє формування даних на стороні пристрою. Ефективність виконання цієї задачі в значній мірі залежить від способу обробки та організації даних на стороні IoT-вузла. Первинні аналогові сигнали, отримані від п'єзокерамічного датчика, потребують початкової обробки: фільтрації високочастотних шумів, нормалізації до відповідного діапазону та, за потреби, обчислення певних показників, наприклад, амплітуди або частоти. Після цього дані перетворюються у відповідний формат для передачі. У сучасних IoT-системах найчастіше застосовуються формати JSON (зручний

для читання та інтеграції), CSV (простий для зберігання) або бінарні структури (оптимальні за розміром).

Зважаючи на обмежені ресурси мікроконтролерів та можливі перебої у з'єднанні, часто застосовується буферизація даних - тимчасове збереження масиву повідомлень у пам'яті пристрою з подальшим пакетним надсиланням у хмару з визначеною періодичністю. Такий підхід дозволяє оптимізувати використання мережевих ресурсів, знизити енергоспоживання та підвищити надійність доставки інформації до AWS.

Вибір протоколів зв'язку для інтеграції з хмарою AWS. У процесі побудови IoT-системи з передачею даних до хмарної інфраструктури AWS важливу роль відіграє вибір мережевого протоколу, який забезпечує ефективну та надійну доставку даних від пристрою до хмари. У практиці IoT найбільш поширеними є протоколи MQTT, HTTPS та WebSocket, які відрізняються за архітектурною моделлю, енергоспоживанням та вимогами до мережевого середовища.

Для систем, що базуються на п'єзокерамічних сенсорах, особливо в умовах обмежених ресурсів або періодичної передачі невеликих обсягів даних, найбільш доцільним є використання MQTT — легковагового протоколу з підтримкою механізму публікації-підписки та мінімальним накладним навантаженням. Протокол HTTPS частіше застосовується в системах з високим рівнем безпеки або для одноразової передачі даних (наприклад, через REST API), тоді як WebSocket використовується у випадках, коли потрібен двосторонній обмін даними в реальному часі (наприклад, моніторинг або керування пристроями).

У таблиці 1 представлено порівняння згаданих протоколів за ключовими критеріями.

Таблиця 1. Порівняння протоколів зв'язку для IoT-пристроїв

Критерій	MQTT	HTTPS	WebSocket
Модель зв'язку	Публікація/підписка	Клієнт-сервер	Двостороннє з'єднання
Накладні витрати	Низькі	Середні	Середні
Енергоспоживання	Низьке	Високе	Середнє
Відповідні сервіси AWS	AWS IoT Core	REST API (API Gateway)	AWS IoT Core
Надійність доставки	Так (QoS 0–2)	Так	Залежить від застосування
Сценарії використання	Сенсори, телеметрія	Одноразові запити, REST	Моніторинг, керування

AWS надає офіційну підтримку MQTT та HTTPS через AWS IoT Device SDK, доступний для таких платформ, як ESP32, STM32, Raspberry Pi тощо. Реалізація зв'язку здійснюється через вбудовані бібліотеки з підтримкою TLS-шифрування, сертифікатів X.509 та MQTT-брокерів, що дозволяє швидко розгорнути захищене з'єднання між пристроєм і хмарою [7].

Якщо брати до уваги особливості п'єзокерамічних датчиків, які зазвичай генерують короткі, але часті вимірювання, та враховуючи обмежені ресурси IoT-пристроїв, найбільш доцільним є використання протоколу MQTT. Його низьке енергоспоживання, підтримка гарантованої доставки (QoS) і сумісність з сервісом AWS IoT Core роблять його оптимальним вибором для передачі даних з п'єзодатчиків у хмарну інфраструктуру AWS.

Інтеграція з хмарною інфраструктурою AWS. Інтеграція IoT-систем, що базуються на п'єзокерамічних датчиках, з хмарними платформами потребує побудови надійної, масштабованої та безпечної архітектури. Важливо не лише забезпечити доставку даних у хмару, а й вибрати оптимальні сервіси для їх обробки, зберігання та подальшого аналізу. При використанні хмарного провайдера AWS для цього доцільно використовувати комбінацію сервісів AWS IoT Core, AWS Lambda, Amazon Timestream, DynamoDB та S3.

На рис. 2 представлено узагальнену схему архітектури інтеграції IoT-пристроїв з п'єзокерамічними датчиками у хмарну інфраструктуру AWS. Вона показує послідовність руху даних: від пристрою через IoT Core та Lambda до сховищ, залежно від обраного сценарію зберігання.

Дані надходять до AWS IoT Core, де автентифікуються і маршрутизуються до AWS Lambda для обробки подій. Оброблені дані зберігаються у відповідному сервісі: Amazon Timestream (часові ряди), Amazon S3 (файлове сховище) або Amazon DynamoDB (оперативна база даних).

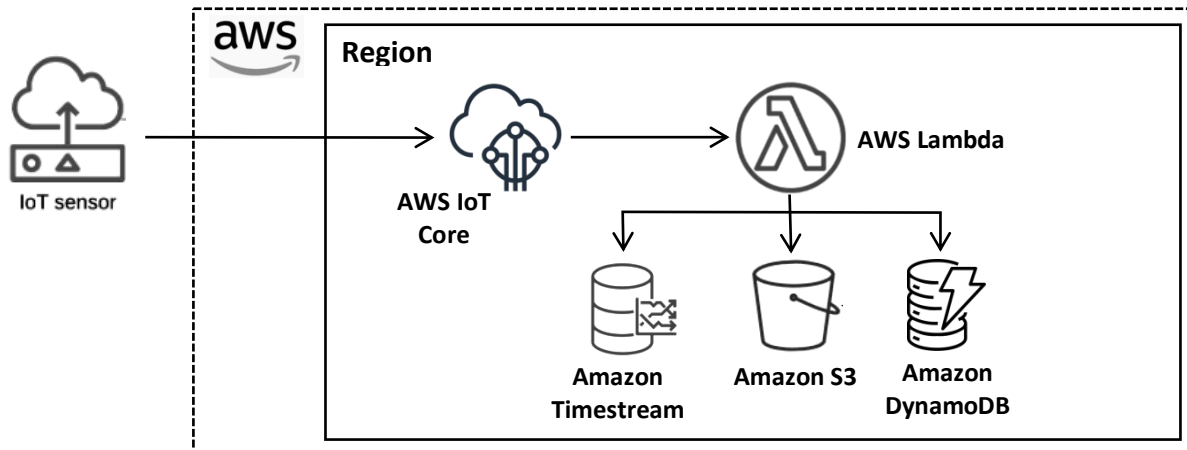


Рис. 2. Схема інтеграції IoT-пристрою у хмарну інфраструктуру AWS

Першим компонентом у ланцюжку інтеграції виступає AWS IoT Core - керований брокер повідомлень, який приймає дані з пристроїв через протоколи MQTT, WebSocket або HTTPS. IoT-пристрої з п'єзокерамічними датчиками, як правило, генерують періодичні вимірювання (наприклад, амплітуди вібрацій), які передаються у вигляді структурованих JSON-повідомлень. Завдяки підтримці MQTT і QoS-рівнів, AWS IoT Core забезпечує гарантовану доставку навіть при нестабільному зв'язку.

Для того щоб підключити п'єзокерамічний IoT-пристрій до AWS IoT Core, необхідно реалізувати автентифікацію пристрою. Це здійснюється за допомогою X.509 сертифікатів, які створюються на платформі AWS і завантажуються в пристрій, або ж через AWS Cognito, що дозволяє реалізувати динамічну автентифікацію з прив'язкою до користувача чи пристрою. Така багаторівнева безпека дозволяє захистити як канал передачі, так і ідентифікацію пристрою в системі.

Після прийому повідомлення на AWS IoT Core, далі в ланцюжку спрацьовує AWS Lambda - serverless-функція, яка виконується автоматично без потреби у виділеному сервері. AWS Lambda може виконувати первинну обробку даних: фільтрацію, нормалізацію, агрегацію, перетворення формату. Це особливо важливо у випадках, коли п'єзодатчики генерують необроблені дані, які потребують попередньої обробки перед зберіганням. AWS Lambda також дозволяє реалізувати тригери для подій, наприклад - надсилання оповіщень при перевищенні порогового значення вібрації.

Залежно від типу оброблених даних, вони можуть зберігатися в одному з кількох сервісів AWS. Amazon Timestream є оптимальним рішенням для зберігання часових рядів - наприклад, значень вібрації або тиску, з прив'язкою до часової мітки. Якщо потрібне архівне або файлове збереження (наприклад, пакетні CSV або JSON), дані можуть бути спрямовані в Amazon S3. У випадках, коли потрібен швидкий доступ до структурованих даних у форматі ключ-значення (наприклад, останній вимір із кожного пристрою), доцільно використовувати Amazon DynamoDB - масштабовану NoSQL-базу з низькою затримкою.

Завдяки масштабованості та розміщенню у кількох зонах доступності (Availability Zones), ця архітектура дозволяє забезпечити достатню надійність та відмовостійкість IoT-системи. У разі збою одного дата-центру, сервіси AWS автоматично перемикаються на інші доступні зони, що особливо важливо у відповідальних задачах моніторингу конструкцій, виробничих процесів чи інженерних споруд, де застосовуються п'єзокерамічні датчики.

Аналітика, візуалізація та обробка даних у хмарі. Після надходження даних з п'єзокерамічних IoT-пристроїв у хмару AWS, можливе подальше їх використання для аналізу, відображення результатів та інтелектуальної обробки значень вимірювальної інформації. Для опрацювання результатів у режимі реального часу можливе застосування Amazon Kinesis, що

забезпечує потокову аналітику з низькою затримкою. Побудову інтерактивних звітів та дашбордів можна реалізувати за допомогою Amazon QuickSight, який зручно інтегрується з Timestream, DynamoDB та іншими сховищами AWS.

У разі необхідності виконання складнішої обробки даних, включно з прогнозуванням або виявленням аномалій, до роботи можуть бути залучені сервіси машинного навчання, зокрема AWS SageMaker, що дозволяє тренувати, розгортати та масштабувати ML-моделі безпосередньо у хмарному середовищі.

І, нарешті, останній підпункт - *забезпечення безпеки та надійності системи*. Основними напрямками захисту є шифрування даних під час передачі (з використанням TLS), автентифікація пристроїв за допомогою X.509-сертифікатів, а також контроль доступу через політики (IAM). Додатково доцільно використовувати AWS IoT Device Defender для виявлення аномалій і забезпечення відповідності політикам безпеки, а також AWS CloudTrail і Amazon CloudWatch — для моніторингу та аудиту.

Детальний аналіз методів захисту інформації при роботі з п'єзодатчиками в хмарній інфраструктурі AWS, включно з питаннями безпеки на рівні мережі, ізоляції критичних сервісів, управління ключами шифрування (Amazon KMS) та протидії DDoS-атакам (AWS Shield), представлено авторами у роботі [8].

Приклад реалізації. Для експериментальних досліджень була побудована система збору та передачі параметрів вібрації, що реалізована за допомогою п'єзокерамічних датчиків. Для реалізації вібрації був задіяний мотор AMS1141M від Elecrow, в якому здійснене асиметричне навантаження на валу.

В якості п'єзокерамічних датчиків IoT пристроїв були використані асиметричні п'єзоелементи 7BB-12-9 фірми muRata: у складі металевої латуневої пластини діаметром 12 мм з товщиною 0,1 мм, та п'єзоелемента діаметром 9 мм і товщиною 0,12 мм. Вага датчика – 0,143 г, частота резонансу – 9 кГц, ємність – 8 нФ. В схемі накопичення енергії була використана схема на основі чипу LTC3330 Linear Technology.

Передача даних від IoT-пристрою до хмарної інфраструктури AWS здійснювалася за допомогою модуля ESP32-WROOM-32, який підтримує Wi-Fi IEEE 802.11 b/g/n. Обрана платформа забезпечує достатні обчислювальні ресурси для попередньої обробки сигналу з п'єзодатчика, формування MQTT-повідомлення та шифрування даних із використанням TLS.

На стороні хмари була використана інфраструктура AWS у регіоні us-east-1 (Північна Вірджинія) з прив'язкою до зони доступності us-east-1a, що дозволяє забезпечити високу доступність і мінімальну затримку для передачі даних. Основні сервіси включали:

- AWS IoT Core - для прийому MQTT-повідомлень;
- AWS Lambda - для обробки подій та фільтрації значень сигналу;
- Amazon Timestream - для зберігання часових рядів вимірювань вібрації;
- Amazon CloudWatch - для моніторингу функціонування Lambda-функцій.

Для перевірки ефективності побудованої архітектури проводився експеримент з передачею вібраційних даних кожні 2 секунди з оцінкою затримки доставки повідомлень, часу обробки у Lambda-функції та доступності Timestream. Дані використовувалися для побудови тестових аналітичних звітів у Amazon QuickSight. Особливу увагу приділено надійності з'єднання при перериванні Wi-Fi-сигналу, а також перевірці повторного підключення з відновленням MQTT-сесії.

Проведені експерименти показали надійність побудованої IoT-системи збору сенсорних даних на основі п'єзокерамічних датчиків у хмарну інфраструктуру AWS, що говорить про достовірність та ефективність проведених досліджень.

Висновки та перспективи подальших досліджень. У статті були описані методи та засоби побудови IoT-системи збору сенсорних даних з п'єзокерамічних датчиків із подальшою інтеграцією в хмарну інфраструктуру AWS. Проаналізовано вибір протоколів зв'язку, структуру обробки подій та зберігання даних у сервісах AWS. Значну увагу приділено практичній реалізації прототипу системи на основі ESP32-модуля з використанням MQTT та AWS IoT Core. Проведені експерименти підтвердили ефективність обраного підходу та його придатність для застосування у задачах моніторингу.

Перспективи подальших досліджень полягають у розширенні аналітичних можливостей системи за допомогою сервісів машинного навчання AWS SageMaker, вивченні можливостей багатовимірної синхронізації, а також адаптації архітектури до умов обмеженого

енергоспоживання з використанням енергоефективних протоколів та механізмів енергозбору (energy harvesting) для автономних IoT-вузлів.

Список бібліографічного опису

1. Nazir S., Poorun Y., Kaleem M. Person detection with deep learning and IoT for smart home security on Amazon Cloud. 2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), 7 October 2021. URL: <https://surl.lu/lhlxhe> (дата звернення: 12.05.2025).
2. Cloud Computing for IoT Sensing Data / D. Kumar та ін. New York : IGI Global Scientific Publishing, 2024. 23 с. URL: <https://surli.cc/ihutnv> (дата звернення: 12.05.2025).
3. Kaarthik K., Vajpayee A. Build a sensor network using AWS IoT Core and Amazon DocumentDB. Amazon Web Services. URL: <https://surli.cc/gdtgrt> (дата звернення: 12.05.2025).
4. Architecture for managing IoT sensor data. Amazon Web Services. URL: <https://surl.li/evwstj> (дата звернення: 12.05.2025).
5. AWS IoT Core. Murata Manufacturing Co. URL: <https://surl.li/btqtvy> (дата звернення: 12.05.2025).
6. Holzel G. IoT Sensor Data Processing Pipeline. GitHub, Inc. URL: <https://surl.li/hjzeod> (дата звернення: 12.05.2025).
7. Device communication protocols. Amazon Web Services. URL: <https://surl.li/dqvxik> (дата звернення: 12.05.2025).
8. Мусієнко М.П., Мусієнко О.Ю. Методи захисту інформації в хмарах AWS при роботі із пристроями IoT на базі п'єзодатчиків // Матеріали доповідей Всеукраїнської науково-практичної Internet-конференції «Автоматизація та комп'ютерно-інтегровані технології у виробництві та освіті: стан, досягнення, перспективи розвитку». – 17-21 березня 2025 року, - Черкаси: ЧНУ ім. Б.Хмельницького. – С. 49-50

References

1. Nazir S., Poorun Y., Kaleem M. Person detection with deep learning and IoT for smart home security on Amazon Cloud. 2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), 7 October 2021. URL: <https://surl.lu/lhlxhe> (access data: 12.05.2025).
2. Cloud Computing for IoT Sensing Data / D. Kumar et al. New York : IGI Global Scientific Publishing, 2024. 23 p. URL: <https://surli.cc/ihutnv> (access date: 12.05.2025).
3. Kaarthik K., Vajpayee A. Build a sensor network using AWS IoT Core and Amazon DocumentDB. Amazon Web Services. URL: <https://surli.cc/gdtgrt> (access date: 12.05.2025).
4. Architecture for managing IoT sensor data. Amazon Web Services. URL: <https://surl.li/evwstj> (access date: 12.05.2025).
5. AWS IoT Core. Murata Manufacturing Co. URL: <https://surl.li/btqtvy> (access date: 12.05.2025).
6. Holzel G. IoT Sensor Data Processing Pipeline. GitHub, Inc. URL: <https://surl.li/hjzeod> (access date: 12.05.2025).
7. Device communication protocols. Amazon Web Services. URL: <https://surl.li/dqvxik> (access date: 12.05.2025).
8. Musiyenko M.P., Musiyenko O.Yu. Methods of information protection in AWS cloud when working with IoT devices based on piezoelectric sensors. Proceedings of the All-Ukrainian Scientific and Practical Internet Conference "Automation and Computer-Integrated Technologies in Industry and Education: State, Achievements, Development Prospects", March 17–21, 2025. – Cherkasy: Bohdan Khmelnytsky National University of Cherkasy. – P. 49–50.