



DOI 10.28925/2663-4023.2025.31.1003

УДК 004.8

Кукулевський Іван Олегович

аспірант

Державний університет "Київський авіаційний інститут", Київ, Україна

ORCID: 0000-0002-2830-3607

ivan.kukulevskiy@outlook.com

Сокирка Євгеній Олександрович

аспірант

Державний університет "Київський авіаційний інститут", Київ, Україна

ORCID: 0000-0003-2356-7213

sokyrka_evgeniy@yahoo.com

Толбатов Андрій Володимирович

к.т.н., доцент, докторант факультету кібербезпеки, комп'ютерної та програмної інженерії

Державний університет "Київський авіаційний інститут", Київ, Україна

ORCID: 0000-0002-9785-9975

tolbatov@ukr.net

ХМАРНІ ПЛАТФОРМИ ЯК КЛЮЧ ДО ЕФЕКТИВНОГО ЗБЕРІГАННЯ ТА АНАЛІЗУ ІОТ-ДАНИХ

Анотація. Стрімкий розвиток Інтернету речей (IoT) спричинив суттєве зростання обсягів даних, що генеруються пристроями, сенсорами та автоматизованими системами. Це створює потребу у високопродуктивних рішеннях для їх зберігання, обробки та аналітики в реальному часі. Традиційні серверні інфраструктури виявилися недостатньо гнучкими й затратними, тому все більше організацій переходять до використання хмарних платформ, які забезпечують масштабованість, надійність і інтеграцію з інструментами машинного навчання. У статті проведено аналіз ключових можливостей провідних хмарних провайдерів: Amazon Web Services (AWS), Microsoft Azure та Google Cloud Platform (GCP) у контексті побудови IoT-рішень. Розглянуто їхні сервіси для підключення пристроїв, потокової обробки даних, аналітики, безпеки та візуалізації. Порівняльна оцінка платформ за критеріями масштабованості, інтеграції, безпеки, аналітичних можливостей і вартості показала, що AWS і Azure мають найвищі загальні показники ефективності (8.375 балів), тоді як GCP вирізняється швидкістю аналітики завдяки сервісам BigQuery і Dataflow. На основі аналізу запропоновано універсальну модель розгортання IoT-рішень у хмарному середовищі, що охоплює етапи підключення пристроїв, передачі даних, їхнього зберігання, потокової обробки, аналітики та візуалізації. Практичний приклад промислової системи моніторингу показує, як поєднання хмарних сервісів і алгоритмів машинного навчання дозволяє виявляти аномалії у роботі обладнання та запобігати простою виробництва. Отримані результати доводять, що хмарні технології є ключовим чинником підвищення ефективності IoT-систем, забезпечуючи оптимальний баланс між масштабованістю, безпекою та економічною доцільністю. Запропонований підхід може бути використаний для побудови гнучких і безпечних рішень у промисловості, транспорті, енергетиці та «розумних» містах.

Ключові слова: Інтернет речей (IoT); хмарні обчислення; аналітика даних; машинне навчання; AWS; Azure; GCP; масштабованість; безпека; промисловий моніторинг.

ВСТУП

Інтенсивний розвиток цифрових технологій та концепції Інтернету речей (IoT) зумовив появу нових підходів до збору, обробки та аналізу даних із розподілених джерел. Сучасні системи генерують значні обсяги інформації, що потребують ефективного управління,



безпечного зберігання та масштабованої інфраструктури. Хмарні технології стали ключовим інструментом у реалізації таких рішень, забезпечуючи високу гнучкість, доступність і інтеграцію з аналітичними сервісами. Водночас зростає потреба у системному підході до вибору та оптимізації хмарних платформ для обробки IoT-даних, що визначає актуальність подальших досліджень у цій сфері.

Постановка проблеми. Розвиток інформаційних технологій та діджиталізація усіх галузей економіки призвели до стрімкого зростання популярності Інтернету речей (Internet of Things, IoT). Сучасні IoT-рішення дозволяють збирати та обробляти величезні обсяги даних від датчиків, пристроїв та систем у реальному часі. Однак одночасно із цим виникають значні виклики, зокрема: зберігання великих масивів інформації, її оперативна обробка та аналіз, забезпечення безпеки тощо [8].

У відповідь на ці виклики розробляються і впроваджуються хмарні платформи, що надають гнучкі та масштабовані ресурси для зберігання і аналізу даних. Такі платформи не лише позбавляють користувачів необхідності утримувати дорогі серверні приміщення, але й забезпечують широкий спектр інструментів для аналітики, машинного навчання, моніторингу та інтеграції з іншими сервісами. Таким чином, питання ефективного вибору та використання хмарних платформ для зберігання та аналізу IoT-даних набуває все більшої актуальності і має як наукову, так і практичну цінність.

Аналіз останніх досліджень і публікацій. Ринок хмарних платформ для зберігання та аналізу IoT-даних в останні роки динамічно зростає [9]. Серед усіх доступних рішень можна виділити три найбільших гравці, які найбільше використовуються у корпоративному сегменті, а також активно впроваджуються у науково-дослідницьких проектах. Для ілюстрації зростання кількості IoT-підключень на найпопулярніших платформах AWS, Azure та GCP наведено в табл. 1. У ній відображено дані стосовно кількості активних IoT-девайсів у період 2022–2024 рр [1-3].

Таблиця 1

Статистика використання IoT-девайсів на хмарних платформах

Рік	AWS IoT (млн. підключень)	Azure IoT (млн. підключень)	GCP IoT (млн. підключень)
2022	45	38	30
2023	52	45	34
2024	58	52	38

На рис. 1 показано динаміку змін цих показників у вигляді стовпчикової діаграми, що дає змогу візуально порівняти зростання на кожній платформі.

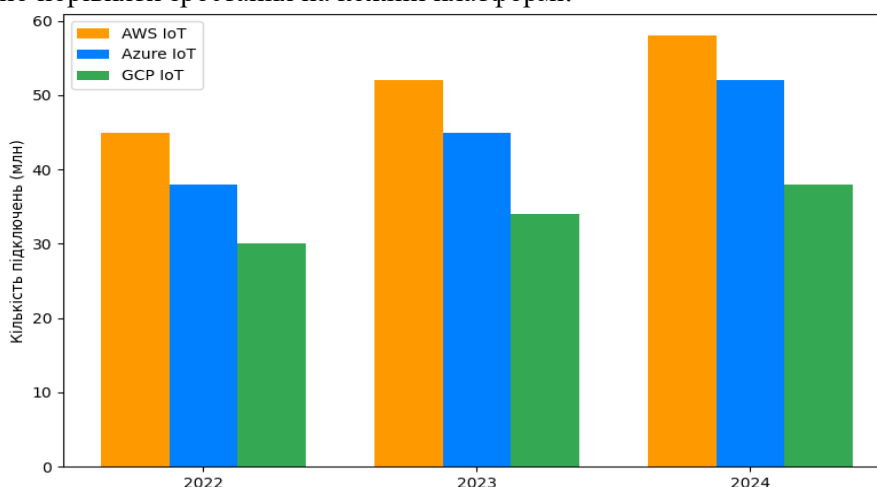


Рис. 1. Аналітика використання IoT-девайсів (2022-2024)



Як видно з табл. 1 та рис. 1, найбільша кількість підключень припадає на платформу AWS, що частково пояснюється її широкою географічною присутністю та різноманітністю сервісів. Проте з року в рік зростають і показники Azure та GCP, що свідчить про конкурентоспроможність рішень Microsoft і Google на ринку хмарних технологій.

Amazon Web Services (AWS) надає потужні можливості для підключення та керування IoT-пристроями через сервіс AWS IoT Core [1]. Цей сервіс забезпечує високошвидкісну обробку мільярдів повідомлень за секунду та інтегрується з іншими сервісами AWS, такими як AWS Lambda для безсерверних обчислень, Amazon Kinesis для потокової обробки даних і Amazon S3 для зберігання об'єктів. Для забезпечення безпеки користувачі можуть налаштовувати політики доступу, застосовувати шифрування даних під час зберігання та передачі, а також використовувати інструменти на кшталт AWS Identity and Access Management (IAM) та AWS IoT Device Defender. AWS пропонує розширені можливості для аналітики та машинного навчання, включаючи Amazon QuickSight, AWS Glue та AWS Lake Formation. Спеціалізований сервіс Amazon Lookout for Equipment дозволяє виявляти аномалії в промисловому обладнанні. Завдяки найбільшій мережі дата-центрів у світі AWS забезпечує мінімальні затримки та високу відмовостійкість. Ключовими перевагами платформи є масштабованість, широкий вибір спеціалізованих сервісів і активна спільнота. Однак складність налаштувань може створювати труднощі для новачків, а вартість використання при великих обсягах даних іноді перевищує витрати на конкурентні рішення.

Microsoft Azure пропонує широкий набір сервісів для роботи з IoT, аналітикою та машинним навчанням. Azure IoT Hub забезпечує безпечне та надійне підключення IoT-пристроїв, підтримуючи двосторонню комунікацію та можливість відправлення оновлень прошивки або команд безпосередньо на пристрої [2]. Для потокової аналітики та обробки даних у режимі реального часу використовується Azure Stream Analytics, який підтримує складні аналітичні запити завдяки SQL-подібному синтаксису. Додаткові можливості для обробки великих даних надають HDInsight (Hadoop/Spark) та Databricks. Azure Machine Learning – це комплексний сервіс для розгортання, навчання та керування моделями машинного навчання, який легко інтегрується з Azure IoT Edge, дозволяючи виконувати аналітику безпосередньо на пристроях. Для візуалізації даних використовується Power BI, що дає змогу створювати інтерактивні дашборди та звіти з підтримкою численних джерел даних. Безпека та управління в Azure реалізовані через Azure Active Directory (Azure AD), який забезпечує ідентифікацію та контроль доступу. Додатковий рівень захисту забезпечує Azure Security Center, який аналізує вразливості та надає рекомендації щодо покращення безпеки. Основними перевагами Azure є тісна інтеграція з екосистемою Microsoft, зручні інструменти для розробників, такі як Visual Studio та GitHub, а також потужні сервіси аналітики. Серед можливих недоліків – менша кількість регіонів порівняно з AWS і складніше налаштування для масштабних сценаріїв Big Data без попереднього досвіду.

Google Cloud Platform (GCP) забезпечує потужні можливості для роботи з IoT, аналітикою та машинним навчанням. Google Cloud IoT Core дозволяє підключати пристрої та збирати дані за допомогою протоколів MQTT і HTTP, маючи вбудовані механізми аутентифікації та шифрування [3]. Для обробки даних використовується Google Cloud Dataflow, який, будучи побудованим на Apache Beam, дозволяє створювати конвеєри для потокової та пакетної обробки. BigQuery є однією з найшвидших аналітичних СУБД, що підтримує інтерактивні SQL-запити до великих обсягів даних. У сфері машинного навчання Vertex AI пропонує комплексну платформу для розробки та впровадження ML-моделей, включаючи AutoML для автоматизованого створення моделей класифікації, регресії та обробки зображень. GCP має високопродуктивну мережеву інфраструктуру, гнучке ціноутворення та зручні інструменти для спільної роботи. Google Kubernetes Engine (GKE) значно спрощує управління контейнерами, забезпечуючи масштабованість та автоматизацію. Безпека реалізована через механізми Identity and Access Management (IAM), Cloud Security Command Center та вбудоване шифрування даних. Google також відомий високим рівнем фізичної безпеки своїх дата-центрів. Серед ключових переваг GCP – надшвидка аналітика у BigQuery, гармонійна інтеграція з іншими Google-сервісами та



зручний користувацький інтерфейс. Можливими недоліками є менша кількість готових спеціалізованих IoT-модулів порівняно з AWS і Azure, хоча основні функції для IoT-застосувань повністю підтримуються.

Таким чином, AWS, Azure і GCP пропонують подібний набір базових можливостей (підключення пристроїв, зберігання даних, аналітика, машинне навчання), але кожна платформа має свої «сильні сторони». AWS орієнтований на широку екосистему та найбільшу регіональну присутність [1]. Azure вигідно інтегрується з Microsoft-продуктами, що особливо зручно для корпоративного середовища Windows [2]. GCP переважає у швидкій обробці великих даних завдяки BigQuery і Dataflow [3]. У виборі рішення варто враховувати конкретні потреби проекту, включаючи вимоги щодо географії, безпеки, бюджету й наявних компетенцій розробників.

IoT-рішення передбачають обробку великих обсягів інформації від розмаїтих пристроїв, що вимагає ретельного планування інфраструктури та методів аналізу даних. Нижче наведено ключові вимоги, які слід врахувати при розробці і впровадженні систем зберігання й аналізу IoT-даних. Масштабованість передбачає можливість гнучкого розширення системи, що дозволяє динамічно збільшувати або зменшувати обчислювальні ресурси, сховища та пропускну здатність відповідно до зростання кількості пристроїв та обсягів даних. Горизонтальне масштабування реалізується шляхом додавання нових вузлів, тоді як вертикальне передбачає збільшення потужності вже існуючих компонентів. Ефективне використання шардінгу та реплікації баз даних забезпечує рівномірний розподіл навантаження та високу доступність даних [1-3]. Надійність і відмовостійкість критично важливі для безперервної роботи системи. Відмова окремого вузла не повинна спричиняти зупинку всієї інфраструктури, що досягається через мультирегіональну реплікацію та архітектуру без єдиних точок відмови. Регулярне резервне копіювання та наявність механізмів швидкого відновлення допомагають мінімізувати наслідки можливих збоїв. Безпека включає багаторівневі механізми аутентифікації та авторизації, що обмежують доступ відповідно до ролей користувачів та пристроїв. Шифрування даних у процесі передачі та зберігання гарантує їх захист від несанкціонованого доступу. Сегментація мережі дозволяє ізолювати різні потоки даних, а системи виявлення аномалій допомагають оперативно реагувати на можливі загрози [4, 6]. Відповідність галузевим стандартам, таким як HIPAA, PCI DSS та GDPR, є важливою умовою для ряду застосувань [5]. Аналітичні можливості охоплюють потокову обробку даних у реальному часі, що дозволяє швидко реагувати на критичні події, а також глибинний аналіз для виявлення довгострокових трендів. Використання платформ Big Data та машинного навчання сприяє створенню прогнозних моделей, а інтеграція з інструментами візуалізації спрощує аналіз навіть для не технічних користувачів [7-10]. Інтеграція забезпечується через API-орієнтовану архітектуру, що дозволяє з'єднувати IoT-платформи з іншими корпоративними системами, такими як CRM та ERP. Гнучка підтримка різних протоколів та форматів дозволяє працювати з широким спектром IoT-пристроїв, включаючи застарілі технології. Економічна доцільність визначається моделлю оплати за фактичне використання ресурсів, що дозволяє оптимізувати витрати. Оцінка сукупної вартості володіння включає не лише оплату за хмарні сервіси, а й витрати на розробку, адміністрування та навчання персоналу. Автоматичне керування ресурсами, моделі резервування та знижки сприяють зниженню витрат при довгостроковому використанні інфраструктури. Врахування усіх перелічених вимог допомагає забезпечити якісний дизайн IoT-рішення, що витримує велике навантаження, є захищеним і здатним вирішувати широкий спектр аналітичних задач у реальному часі або в режимі глибинного аналізу [5-7].

Для об'єктивного порівняння хмарних платформ було розроблено систему оцінювання за десятибальною шкалою (від 0 до 10). Оцінки базуються на аналізі офіційної документації провайдерів [1-3], відгуках користувачів, незалежних дослідженнях ринку та тестуванні основних сервісів. Інтерпретація оцінок:

- 0–3 – обмежена функціональність або висока складність у впровадженні.
- 4–6 – середній рівень можливостей, які потребують додаткових налаштувань.
- 7–8 – добре розвинені інструменти та сервіси, але можуть мати певні обмеження.



- 9–10 – провідне рішення у своїй категорії з високою продуктивністю, зручністю та гнучкістю.

Вагові коефіцієнти для кожного критерію визначалися відповідно до їхнього впливу на ефективність IoT-рішення:

- Масштабованість – 0.2
- Аналітичні можливості – 0.2
- Безпека – 0.15
- Інтеграція з іншими сервісами – 0.15
- Ціноутворення та гнучкість тарифів – 0.1
- Простота налаштування – 0.1
- Географічна присутність – 0.05
- Спеціалізовані IoT-сервіси – 0.05

Результати порівняння представлені у таблиці:

Таблиця 2

Порівняльна таблиця хмарних платформ для IoT рішень

Критерій	Вага	AWS	Azure	GCP
Масштабованість	0.2	10	9	8
Аналітичні можливості	0.2	9	8	10
Безпека	0.15	9	9	8
Інтеграція з іншими сервісами	0.15	8	10	9
Ціноутворення та гнучкість тарифів	0.1	6	7	9
Простота налаштування	0.1	6	7	8
Географічна присутність	0.05	10	8	7
Спеціалізовані IoT-сервіси	0.05	9	9	7
Зважена оцінка	-	8.375	8.375	8.25

AWS отримав найвищий бал за масштабованість (найбільша хмарна інфраструктура) та географічну присутність, що робить його лідером у розгортанні глобальних IoT-рішень [1]. GCP переважає в аналітичних можливостях, оскільки його сервіси BigQuery та Dataflow [3] забезпечують ефективну обробку великих потоків даних у реальному часі. Azure має найкращу інтеграцію з корпоративними продуктами, зокрема із системами Microsoft [2], що полегшує взаємодію з наявною інфраструктурою підприємств. Також варто враховувати гнучкість цінових моделей: GCP пропонує вигідніші тарифи для масштабованих аналітичних завдань, тоді як AWS може бути дорожчим при високих обсягах обробки. У свою чергу, Azure забезпечує баланс між вартістю та функціональністю. Загальна підсумкова оцінка платформ, обчислена на основі зваженої середньої оцінок за критеріями, виглядає так:

- AWS: 8.375
- Azure: 8.375
- GCP: 8.25

Таким чином, AWS та Azure демонструють приблизно однаковий рівень ефективності, але з різним фокусом (рис. 2). AWS підходить для масштабних глобальних рішень, Azure – для інтеграції з екосистемою Microsoft. GCP дещо поступається за масштабованістю, але перевершує конкурентів у швидкій аналітиці великих даних. У виборі рішення варто враховувати конкретні потреби проекту, включаючи вимоги щодо географії, безпеки, бюджету й наявних компетенцій розробників.

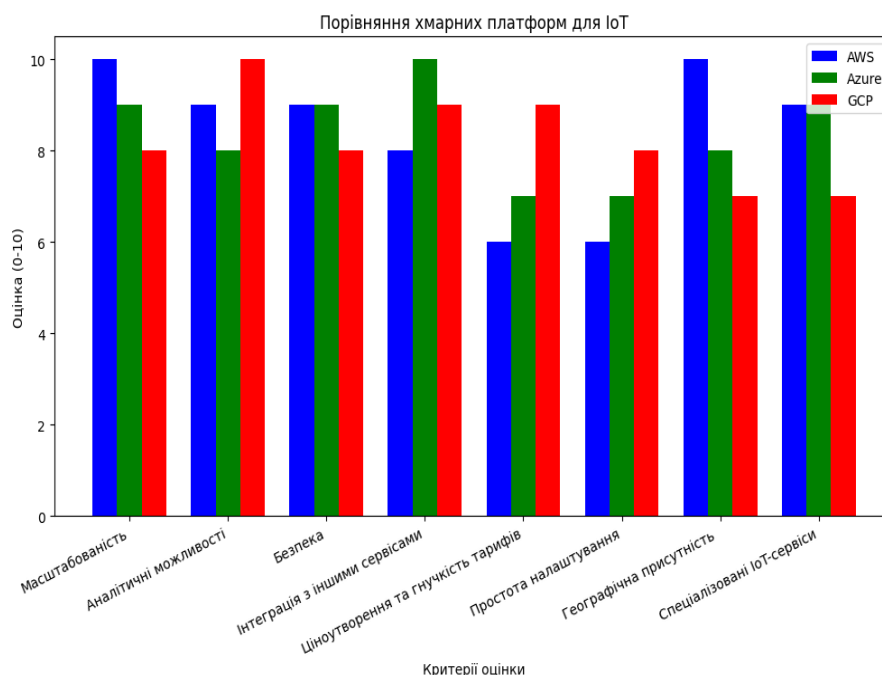


Рис. 2. Порівняння хмарних платформ для IoT рішень

Мета статті. Стаття зосереджується на аналізі ключових особливостей найпопулярніших хмарних платформ, що використовуються для реалізації IoT-рішень [1-3]. Основна увага приділяється визначенню критеріїв вибору платформи залежно від специфіки конкретного проєкту. Також розглядається розробка універсальної моделі, яка передбачає покроковий підхід до розгортання IoT-рішення у хмарі - від етапу підключення пристроїв до подальшої аналітики та візуалізації даних. Для практичної демонстрації теоретичних положень наводиться реалістичний приклад використання однієї з хмарних платформ у типовому IoT-сценарії.

ОСНОВНА ЧАСТИНА ДОСЛІДЖЕННЯ

Виклад основного матеріалу. Типове IoT-рішення в хмарному середовищі складається з кількох основних компонентів, кожен з яких виконує важливу функцію. На початковому рівні працюють IoT-пристрої, такі як датчики, контролери та «розумні» пристрої, що здійснюють збір даних [7]. Передача цих даних у хмару відбувається через шлюзи або брокери повідомлень із використанням безпечних протоколів, зокрема MQTT чи HTTPS. На наступному етапі відбувається обробка інформації за допомогою спеціалізованих сервісів, серед яких IoT Core, функції без сервера, потокова аналітика та черги повідомлень. Вони забезпечують приймання, фільтрацію та розподіл даних відповідно до потреб системи. Збереження великих обсягів інформації здійснюється в базах даних, об'єктних сховищах або дата-лейках, що дозволяє довготривале зберігання та подальший аналіз [2]. Дані, що надходять, можуть бути оброблені за допомогою аналітичних сервісів, які включають інструменти для роботи з Big Data, модулі машинного навчання та засоби візуалізації. Вони допомагають будувати прогнози та знаходити закономірності у великих масивах інформації. Кінцевим рівнем є застосунки та панелі управління, де користувачі можуть взаємодіяти із системою, здійснювати моніторинг, аналізувати дані та керувати пристроями. Оскільки провайдери хмарних послуг пропонують схожі модулі для реалізації IoT-рішень, ключовими аспектами є сумісність між ними та правильна конфігурація відповідно до конкретних завдань. При виборі хмарної платформи для IoT-рішення необхідно враховувати кілька ключових аспектів. Перш за все, важливо, щоб платформа підтримувала необхідні протоколи та стандарти, оскільки специфічні вимоги до

протоколів можуть істотно вплинути на прийняття рішення. Також слід звернути увагу на масштабованість платформи. Оскільки IoT-проекти часто передбачають швидке зростання кількості пристроїв і обсягів даних, важливо, щоб платформа могла ефективно масштабуватися для задоволення цих потреб. Не менш важливими є аспекти безпеки та конфіденційності. Платформа повинна відповідати міжнародним стандартам безпеки, таким як ISO 27001, та забезпечувати шифрування даних і відповідність нормам, наприклад, GDPR. Крім того, доступність дата-центрів у потрібних регіонах може впливати на затримки та швидкість роботи платформи, що також має бути враховано. Вартість використання платформи є важливим фактором, оскільки різні моделі ціноутворення можуть значно вплинути на бюджет проекту. Оцінка витрат на зберігання даних, кількість повідомлень і операцій важлива для того, щоб уникнути несподіваних витрат. Інструменти для аналітики також мають велике значення. Наявність сервісів для потокової обробки даних, машинного навчання та візуалізації значно спрощує процес розробки і впровадження рішень [4-5]. Нарешті, важливим є супровід та технічна підтримка. Наявність сервіс-леเวล угоди (SLA), підтримка 24/7 і активна спільнота розробників сприяють швидкому вирішенню проблем і підтримці безперервної роботи системи.

Універсальна модель побудови IoT-рішення в хмарі передбачає кілька етапів, кожен з яких орієнтований на конкретні потреби проекту (рис. 3). Спочатку необхідно визначити функціональні та нефункціональні вимоги, такі як кількість пристроїв, типи даних, рівень безпеки тощо, а також провести дослідження можливих платформ на основі заздалегідь визначених критеріїв. Після цього реєструється обліковий запис у вибраного постачальника хмарних послуг, і налаштовуються основні сервіси, включаючи IoT Core, бази даних і системи безпеки. Організовується мережева структура, налаштовуються VPC, підмережі та брандмауери. Після створення середовища у хмарі визначаються типи даних (структуровані, неструктуровані, потокові), обираються відповідні технології для їхнього зберігання, а також налаштовуються механізми резервного копіювання і відновлення. Наступним кроком є налаштування механізмів обробки та аналітики: для потокової обробки даних у реальному часі використовуються сервіси, такі як AWS Kinesis або GCP Dataflow, а для довготривалої аналітики застосовуються інструменти Big Data та машинного навчання. Після цього організовується візуалізація даних на дашбордах та налаштовуються інтерфейси для доступу до результатів. На завершення проводяться тестування, перевірка на навантаження та впровадження системи в продуктивне середовище з подальшим моніторингом.



Рис. 3. Покрокова модель побудови IoT-рішення в хмарі

Припустимо, що на промисловому підприємстві необхідно контролювати стан обладнання для підвищення ефективності виробництва та попередження відмов верстатів. Для цього система збирає в реальному часі дані з десятків або сотень датчиків на кожному верстаті, такі як температура, вібрація, рівень шуму та споживання електроенергії. Ці дані надходять до шлюзу через MQTT або HTTPS, після чого передаються в хмарну платформу, де зберігається інформація про кожен пристрій. Дані, що надходять на платформу, спочатку фільтруються та валідуються, після чого потрапляють у механізм потокової аналітики для відстеження метрик, таких як середня температура чи частота пікових вібрацій. Якщо значення перевищують критичні пороги, система генерує події, що сповіщають операторів. Одночасно ці дані можуть зберігатися в хмарному сховищі, що дозволяє здійснювати глибинний аналіз і формувати історичні тренди. Зібрані дані можуть бути використані для розгортання моделі машинного навчання, яка на основі аналізу температури, вібрації та інших факторів здатна виявляти аномалії в роботі обладнання.



Модель постійно оновлюється для підвищення точності прогнозів. При виявленні аномалії система автоматично генерує попередження, що дозволяє заздалегідь планувати технічне обслуговування. Дані з хмарного сховища виводяться на аналітичні панелі, де оператори можуть переглядати графіки, теплові карти та порівняння різних верстатів. Система також надає рольовий доступ до аналітики, де технічні фахівці можуть бачити детальну інформацію про передбачені відмови, а керівники, загальний стан виробництва. У разі виявлення аномалії система може автоматично створити завдання в ERP або MES для повідомлення інженерів про необхідність перевірки обладнання. Якщо показники наближаються до критичних значень, система може зупинити верстат, щоб уникнути аварії [7]. Завдяки такій інтеграції, оператори отримують лише найбільш термінові сповіщення, а система машинного навчання дозволяє знижувати ризики не запланованих простоїв. Хмарна інфраструктура дає можливість масштабувати рішення без великих інфраструктурних витрат, об'єднуючи дані з різних виробничих ліній для порівняння та оптимізації всього ланцюга постачання.

В межах розглянутого рішення було визначено типову архітектуру IoT-системи в хмарному середовищі й описано ключові етапи, від збору та передачі даних з пристроїв через шлюзи, до налаштування обробки, зберігання та аналітики у хмарній платформі. На реальному прикладі промислового підприємства продемонстровано, як за допомогою хмарних сервісів і машинного навчання можна виявляти аномалії у роботі обладнання, своєчасно реагувати на критичні показники й масштабувати рішення без значних інфраструктурних витрат. Це дозволяє оптимізувати виробничі процеси, підвищити ефективність і мінімізувати тривалість простоїв.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У ході дослідження було здійснено детальний аналіз популярних хмарних платформ для реалізації IoT-рішень, зокрема AWS, Azure та GCP, а також інших провайдерів, що пропонують спеціалізовані інструменти для роботи з великими обсягами даних, потоковою аналітикою та машинним навчанням. Оцінено їхні ключові характеристики, включно з масштабованістю, безпекою, доступністю дата-центрів і вартістю. Порівняльний огляд продемонстрував, що попри схожість базових сервісів (підключення пристроїв, зберігання даних, аналітичні можливості), кожен провайдер має власні «сильні сторони». AWS вирізняється великою географічною присутністю й широким вибором спеціалізованих сервісів, Azure пропонує тісну інтеграцію з продуктами Microsoft, а GCP лідирує у високошвидкісній обробці великих даних завдяки BigQuery та Dataflow.

Одним із центральних результатів є розробка універсального покрокового підходу до побудови IoT-системи у хмарі. Запропонована модель охоплює увесь життєвий цикл, від первинної оцінки вимог та реєстрації в обраного хмарного провайдера, через проектування архітектури зберігання й обробки (з використанням інструментів потокової аналітики та Big Data), і до впровадження системи з подальшим моніторингом, візуалізацією та машинним навчанням. Такий структурований підхід допомагає адаптувати рішення під специфіку конкретного проекту, враховуючи вимоги до безпеки, масштабованості й інструментів аналізу.

На прикладі промислового підприємства продемонстровано практичні переваги запропонованої методики: зокрема, своєчасне виявлення аномалій у роботі обладнання дає змогу запобігти раптовим відмовам, забезпечити планування технічного обслуговування й підвищити загальну ефективність виробництва. Механізми потокової обробки даних та застосування алгоритмів машинного навчання дають змогу не лише накопичувати великі обсяги інформації, а й оперативно перетворювати їх на корисні поради для прийняття управлінських рішень. При цьому рольова модель доступу в системі дозволяє налаштувати різні рівні привілеїв для фахівців технічної сфери та керівників виробничих підрозділів, що спрощує взаємодію з даними.

Узагальнюючи отримані результати, можна зробити висновок, що використання хмарних платформ істотно спрощує реалізацію комплексних IoT-рішень, оскільки звільняє від необхідності розбудови власної фізичної інфраструктури та забезпечує високу гнучкість у виборі технологій зберігання й обробки. Водночас важливо ретельно планувати архітектуру системи та



враховувати ключові критерії вибору провайдера (масштабованість, безпека, аналітичні інструменти, інтеграція з існуючими сервісами, вартість), щоб забезпечити безперебійну й економічно доцільну роботу IoT-рішення. Розглянута модель побудови та практичний приклад її застосування підтверджують доцільність такого підходу у різних галузях, від промисловості та транспорту до міської інфраструктури й сфери послуг, відкриваючи широкі можливості для підвищення ефективності та інноваційного розвитку.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Amazon Web Services. (n.d.). AWS IoT Core. <https://aws.amazon.com/iot-core/>
2. Microsoft Azure. (n.d.). Azure IoT Hub. <https://azure.microsoft.com/en-us/services/iot-hub/>
3. Google Cloud. (n.d.). Google Cloud IoT. <https://cloud.google.com/iot/>
4. International Organization for Standardization. (n.d.). ISO/IEC 27001 — Information security management. <https://www.iso.org/isoiec-27001-information-security.html>
5. Петрів, О. О. (2021). Хмарні обчислення у розвитку Інтернету речей. Сучасні інформаційні системи, (2), 15–22.
6. Сидоренко, В. І. (2022). Безпека в хмарних інфраструктурах IoT. Технології захисту інформації, (3), 47–53.
7. Єременко, П. М. (2023). Машинне навчання у середовищі хмарних платформ. Комп'ютерні науки та кібербезпека, (1), 29–35.
8. Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2020). A survey on IoT security: Application areas, security threats, and solution architectures. IEEE Access, 8, 164769–164798. <https://doi.org/10.1109/ACCESS.2020.3023801>
9. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7), 1645–1660. <https://doi.org/10.1016/j.future.2013.01.010>
10. Kreuzberger, D., Kühl, N., & Satzger, G. (2022). Machine learning operations (MLOps): Overview, definition, and architecture. IEEE Transactions on Artificial Intelligence, 3(5), 646–658. <https://doi.org/10.1109/TAI.2022.3154489>

**Ivan Kukulevskyi**

postgraduate

State University "Kyiv Aviation Institute", Kyiv, Ukraine

ORCID: 0000-0002-2830-3607

*ivan.kukulevskyi@outlook.com***Ievgenii Sokyrka**

postgraduate

State University "Kyiv Aviation Institute", Kyiv, Ukraine

ORCID: 0000-0003-2356-7213

*sokyrka_evgeniy@yahoo.com***Andrii Tolbatov**

PhD, Associate Professor,

Doctoral Researcher at the Faculty of Cybersecurity, Computer and Software Engineering

State University "Kyiv Aviation Institute", Kyiv, Ukraine

ORCID: 0000-0002-9785-9975

tolbatov@ukr.net

CLOUD PLATFORMS AS THE KEY TO EFFECTIVE STORAGE AND ANALYSIS OF IOT DATA

Abstract. The rapid development of the Internet of Things (IoT) has led to a significant increase in the volume of data generated by devices, sensors, and automated systems. This creates a demand for high-performance solutions capable of storing, processing, and analyzing data in real time. Traditional on-premises infrastructures have proven to be inflexible and costly, prompting organizations to migrate toward cloud platforms that provide scalability, reliability, and seamless integration with machine learning tools. The article analyzes the key capabilities of major cloud providers: Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) in the context of IoT solution deployment. It examines their services for device connectivity, data streaming, analytics, security, and visualization. A comparative assessment of these platforms based on scalability, integration, security, analytical capabilities, and cost-efficiency shows that AWS and Azure demonstrate the highest overall performance (8.375 points), while GCP stands out for its analytical speed enabled by BigQuery and Dataflow. Based on the analysis, a universal model for deploying IoT solutions in a cloud environment is proposed. The model includes the stages of device connectivity, data transmission, storage, stream processing, analytics, and visualization. A practical example of an industrial monitoring system demonstrates how the combination of cloud services and machine learning algorithms enables anomaly detection in equipment operation and prevents production downtime. The results confirm that cloud technologies are a key factor in enhancing the efficiency of IoT systems, providing an optimal balance between scalability, security, and cost-effectiveness. The proposed approach can be applied to the design of flexible and secure IoT solutions across various sectors, including industry, transportation, energy, and smart cities.

Keywords: Internet of Things (IoT); cloud computing; data analytics; machine learning; AWS; Azure; GCP; scalability; security; industrial monitoring.

REFERENCES

1. Amazon Web Services. (n.d.). AWS IoT Core. <https://aws.amazon.com/iot-core/>
2. Microsoft Azure. (n.d.). Azure IoT Hub. <https://azure.microsoft.com/en-us/services/iot-hub/>
3. Google Cloud. (n.d.). Google Cloud IoT. <https://cloud.google.com/iot/>
4. International Organization for Standardization. (n.d.). ISO/IEC 27001 — Information security management. <https://www.iso.org/isoiec-27001-information-security.html>
5. Petriv, O. O. (2021). Cloud computing in the development of the Internet of Things. *Modern Information Systems*, (2), 15–22.



6. Sydorenko, V. I. (2022). Security in cloud IoT infrastructures. *Information Protection Technologies*, (3), 47–53.
7. Yeremenko, P. M. (2023). Machine learning in cloud platform environments. *Computer Science and Cybersecurity*, (1), 29–35.
8. Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2020). A survey on IoT security: Application areas, security threats, and solution architectures. *IEEE Access*, 8, 164769–164798. <https://doi.org/10.1109/ACCESS.2020.3023801>
9. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7), 1645–1660. <https://doi.org/10.1016/j.future.2013.01.010>
10. Kreuzberger, D., Kühl, N., & Satzger, G. (2022). Machine learning operations (MLOps): Overview, definition, and architecture. *IEEE Transactions on Artificial Intelligence*, 3(5), 646–658. <https://doi.org/10.1109/TAI.2022.3154489>



This work is licensed under Creative Commons Attribution-noncommercial-sharealike 4.0 International License.