Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет _____Автоматики і комп'ютеризованих технологій_____
(повна назва)

Кафедра ___Комп'ютерно-інтегрованих технологій, автоматизації та робототехніки_
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти _____другий (магістерський)_____
_____Розроблення системи автоматизації для моніторингу та прогнозування стану технологічних процесів_____
(тема)

Виконав:
здобувач _ II-го_ року навчання,
групи ___КІТПВм-23-1_____
_____Канунніков М.Ю._____
(прізвище, ініціали)

Спеціальність ___174 Автоматизація, комп'ютерно - інтегровані технології та робототехніка_____
(код і повна назва спеціальності)
Тип програми ____освітньо-професійна_____
(освітньо-професійна або освітньо-наукова)
Освітня програма __Комп'ютерно-інтегровані_ ___технологічні процеси і виробництва_____
(повна назва освітньої програми)

Керівник ____доц. Сичова О.В._____
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ __Невлюдов І.Ш._
(підпис) (прізвище, ініціали)

2025 р.

Харківський національний університет радіоелектроніки

Факультет____АКТ_____

Кафедра_____КІТАР_____

Рівень вищої освіти_____Другий (магістерський)_____

Спеціальність__174 Автоматизація, комп'ютерно-інтегровані технології та робототехніка

(код і повна назва)

Тип програми _____Освітньо-професійна_____

(освітньо-професійна або освітньо-наукова)

Освітня програма Комп’ютерно-інтегровані технологічні процеси і виробництва

(повна назва)

ЗАТВЕРДЖУЮ:

Зав. кафедри _____

(підпис)

«____»_____ 20 ___ р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві_____Кануннікову Микиті Юрійовичу_____

(прізвище, ім’я, по батькові)

1. Тема роботи _Розроблення системи автоматизації для моніторингу та прогнозування стану технологічних процесів_____

затверджена наказом університету від _22_ _листопада_2024_ р. № __1231Ст_

2. Термін подання здобувачем роботи до екзаменаційної комісії 31_ __січня___ 2025_ р.

3. Вихідні дані до роботи Автоматизувати процес моніторингу та прогнозування стану технологічних процесів, Windows 11, Azure, SQL _____

4.1 Вступ 4.2 Аналіз сучасних систем моніторингу технологічних процесів_____

4.3 Проєктування структури та розробка автоматизованої системи моніторингу_____

4.4 Розроблення симулятора сенсорних даних для моніторингу технологічних процесів___

4.5 Механізм класифікації даних у хмарному середовищі stream analytics

4.6 Експериментальний аналіз роботи системи виявлення аномалій 4.7 Безпека користувачів у системах моніторингу 4.8 Висновки 4.9 Перелік джерел посилання._____

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів). Демонстраційний матеріал представлений у форматі презентації PowerPoint (*.ppt) – 15с. формату А4

6. Консультанти розділів роботи

Найменування розділу	Керівник (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
Пор.	Назва етапів кваліфікаційної роботи	Термін виконання етапів	Примітка
1.	Отримання завдання кваліфікаційної роботи	22.11.2024	Виконано
2.	Аналіз вимог та дослідження предметної області	25.11.2024	Виконано
3.	Визначення ключових цілей і структури проєкту	28.11.2024	Виконано
4.	Проєктування архітектури системи	02.12.2024	Виконано
5.	Реалізація інтеграції компонентів хмарної платформи	06.12.2024	Виконано
6.	Розробка механізмів виявлення аномальних станів	12.12.2024	Виконано
7.	Перевірка працездатності системи на симульованих даних	17.12.2024	Виконано
8	Формування звітності у Power BI та технічної документації	22.12.2024	Виконано
9.	Аналіз безпеки та перевірка відповідності вимога	26.12.2024	Виконано
10	Написання пояснювальної записки	05.01.2025	Виконано
11	Представлення кваліфікаційної роботи	24.01.2025	

Дата видачі завдання __*22 листопада 2024*__ р.

Здобувач _____ _____ *Канунніков М.Ю.*
(підпис)

Керівник роботи _____ *доц. Сичова О.В.*
(підпис) (посада, прізвище, ініціали)

Я як студент ХНУРЕ розумію і підтримую політику закладу із академічної доброчесності. Я не надавав і не одержував недозволену допомогу під час підготовки кваліфікаційної роботи. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

24 січня 2025 р.  *Канунніков М.Ю.*

РЕФЕРАТ

Пояснювальна записка: 68 с., 24 рис., 3 дод., 45 джерел.

СИСТЕМА, МОНІТОРИНГУ, АВТОМАТИЗАЦЯ, INDUSTRY 4.0, AZURE, ХМАРНІ ТЕХНОЛОГІЇ, АНАЛІТИКА

Об'єктом дослідження є процес автоматизації моніторингу та прогнозування стану технологічних процесів.

Предметом дослідження є методи обробки потокових даних для забезпечення ефективного моніторингу технологічних процесів.

Метою дослідження є оптимізація архітектури системи для моніторингу та прогнозування стану технологічних процесів, що включає забезпечення автоматизації аналізу даних і доступу до актуальної інформації в режимі реального часу. Досягнення цієї мети сприятиме підвищенню ефективності управління технологічними процесами та зниженню ризиків можливих збоїв.

Завданням дослідження є створення архітектури системи моніторингу, яка включає інтеграцію ключових компонентів, таких як Azure DPS, BusQueue, Stream Analytics, Azure Storage та Power BI. Важливим аспектом є забезпечення автоматичного реагування на зміни в технологічних процесах шляхом впровадження Logic App. Також до завдань входить тестування інтегрованої архітектури в реальних умовах для оцінки її продуктивності.

Методом дослідження є аналіз і моделювання процесів автоматизації моніторингу та прогнозування, реалізованих на базі хмарної платформи Azure. До методу також входить тестування розробленої архітектури з використанням

синтетичних даних для оцінки її точності, швидкості реагування та адаптивності до умов виробничих процесів.

Вихідними даними для дослідження є телеметрична інформація, отримана від сенсорів, а також дані з різних додаткових джерел, які обробляються та аналізуються на платформі Azure. Це дозволяє забезпечити багатогранний підхід до моніторингу та прогнозування.

Результати виконаної роботи найкраще проявить себе у реальних умовах функціонування технологічних підприємств. Розроблена система дозволяє здійснювати точний моніторинг і своєчасне прогнозування стану технологічних процесів, що сприяє підвищенню ефективності виробництва та забезпеченню стабільності роботи обладнання в режимі реального часу.

Результати кваліфікаційної роботи апробовані під час участі у всеукраїнській студентській конференції, а також опубліковані у збірнику наукових робіт категорії «Б» Переліку наукових фахових видань України, що підтверджує їх наукову цінність і практичну значущість.

Отримані результати дослідження можна віднести до Цілей сталого розвитку 8 «Гідна праця та економічне зростання», а саме до пункту 8.2: «Підвищувати ефективність виробництва на засадах сталого розвитку та розвитку високотехнологічних конкурентних виробництв». Успішна реалізація запропонованих рішень сприятиме створенню стійких і конкурентоспроможних виробничих систем.

ABSTRACT

Explanatory note: 68 p., 24 figures, 3 app. , 45 sources.

SYSTEM MONITORING, AUTOMATION, INDUSTRY 4.0, AZURE, CLOUD TECHNOLOGIES, ANALYTICS

The object of research is the automation of monitoring and forecasting the state of technological processes, which is based on the analysis of data obtained from industrial sensors, IoT devices and data collection systems. These processes play an important role in ensuring the stability and efficiency of modern manufacturing enterprises.

The subject of the study is the development and implementation of methods for collecting, processing and analyzing data within automated monitoring systems.

The aim of the study is to optimize the system architecture for monitoring and forecasting the state of technological processes, including the automation of data analysis and access to up-to-date information in real time. Achieving this goal will help improve the efficiency of process control and reduce the risk of possible failures.

The objective of the study is to create a monitoring system architecture that includes the integration of key components such as Azure DPS, BusQueue, Stream Analytics, Azure Storage, and Power BI. An important aspect is to ensure automatic response to changes in technological processes by implementing Logic App. The tasks also include testing the integrated architecture in real conditions to evaluate its performance.

The research method is the analysis and modeling of automation processes for monitoring and forecasting implemented on the basis of the Azure cloud platform. The method also includes testing the developed architecture using synthetic data to evaluate its accuracy, responsiveness, and adaptability to the conditions of production processes.

The initial data for the study is telemetry information received from sensors, as well as data from various additional sources that are processed and analyzed on the Azure platform. This allows for a multifaceted approach to monitoring and forecasting.

The results of the work performed will be best demonstrated in the real conditions of technological enterprises. The developed system allows for accurate monitoring and timely forecasting of the state of technological processes, which helps to increase production efficiency and ensure the stability of equipment operation in real time.

The results of the qualification work were tested during participation in the All-Ukrainian Student Conference and published in the collection of scientific papers of category «B» of the List of scientific professional publications of Ukraine, which confirms their scientific value and practical significance.

The results of the study can be attributed to Sustainable Development Goal 8 «Decent Work and Economic Growth», namely to paragraph 8.2: «Increase production efficiency on the basis of sustainable development and development of high-tech competitive industries». Successful implementation of the proposed solutions will help create sustainable and competitive production systems.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

ТАУ – наукова дисципліна, що вивчає принципи, методи та алгоритми управління динамічними системами для забезпечення їх стабільності, ефективності та оптимальності. Вона використовується для моделювання, аналізу та розробки систем управління в різних галузях, включаючи автоматизацію технологічних процесів, транспорт, енергетику та робототехніку;

Azure Blob Storage – сервіс хмарного зберігання від Microsoft Azure, що дозволяє зберігати великі обсяги неструктурованих даних, таких як текст або бінарні файли;

IoT (Internet of Things) – мережа взаємопов'язаних пристроїв, що можуть збирати та обмінюватися даними через Інтернет, використовуючи вбудовані датчики, програмне забезпечення та інші технології;

KPI (Key Performance Indicator) – ключові показники ефективності, які використовуються для вимірювання продуктивності процесу або досягнення поставлених цілей;

Logic App – сервіс Microsoft Azure для створення автоматизованих робочих процесів, що дозволяє інтегрувати різні сервіси та автоматизувати робочі процеси без написання коду;

MQTT (Message Queuing Telemetry Transport) – легкий протокол передачі повідомлень, оптимізований для роботи з пристроями IoT, який забезпечує ефективну, надійну та безпечну передачу даних у мережах із низькою пропускною здатністю або високою затримкою;

Power BI – інструмент аналітики даних від Microsoft, що дозволяє збирати, обробляти та візуалізувати дані з різних джерел для прийняття рішень на основі аналітичних звітів;

SCADA (Supervisory Control and Data Acquisition) – система для моніторингу, управління та збору даних з промислових процесів у реальному часі, використовується в автоматизації технологічних процесів.

ВСТУП

Стрімкий розвиток технологічної промисловості та її автоматизації висуває все більш високі вимоги до ефективності, надійності та безперервності роботи технологічних процесів. Цей розвиток торкнувся критичних галузей, таких як військова, нафтогазова, металургійна, хімічна промисловість де стабільність та передбачуваність роботи технологічного обладнання є надважливими аспектом для безперервної роботи виробництв та мінімізації ризиків.

Згідно вищеописаному, традиційні методи моніторингу та прогнозування стану технологічних процесів, які базуються на періодичних перевірках та планових ремонтах стають значно менш ефективними та фактично застарівають. Саме це і є підставою для пошуку нових підходів та застосування їх до процесу моніторингу та прогнозування стану технологічних процесів.

Ключовим напрямком для вирішення цієї проблеми є створення автоматизованої кібер-фізичної системи моніторингу процесів та прогнозування стану технологічних процесів. Автоматизовані системи моніторингу та прогнозування ідеально накладаються на концепт Industry 4.0. Інтеграція таких систем дозволить в режимі наближеному до реального часу отримувати дані про роботу обладнання та відповідним чином класифікувати їх. Варто зауважити, що такі автоматизовані системи дають змогу не тільки збирати дані у близькому до реального часу, а ще й аналізувати їх. Використання подібного підходу, беззаперечно, позитивним чином вплине на будь-яке підприємство забезпечуючи більш ефективне технічне обслуговування з одночасним зниженням експлуатаційних витрат.

Актуальність цієї роботи проявляється у тому, що впровадження автоматизації систем моніторингу та прогнозування є не тільки технічним, а й економічним фактором, яке в більшій мірі впливає на конкурентноспроможність підприємств. Враховуючи потреби міжнародних та українських підприємств однозначно прослідкується тенденція глобалізації, яка передбачає максимальне

оптимізування виробничих процесів. Виходячи з цього імплементація такого підходу є критично важливим аспектом і повинно знаходитись у пріоритеті для виробництв будь якого рівня.

Мета цієї роботи передбачає дослідження та розробку методів автоматизації процесу моніторингу та прогнозування стану технологічних процесів. Найкращим чином розкрити мету вийде побудувавши кібер-фізичну систему, яка дозволить не тільки контролювати стан обладнання в реальному часу, а й робити класифікацію стану обладнання, визначаючи, чи аномально працює приладдя. Це, в свою чергу, дозволить оптимізувати технологічні процеси, забезпечити їх безперебійну роботу та знизити витрати на експлуатацію обладнання.

Область застосування розроблених методів та рішень полягає у цілому спектрі промислових виробництв, де стабільність та ефективність роботи обладнання є критично важливими. Можливість зниження економічних витрат робить доцільним імплементацію подібних методів та рішень для кожного виробництва середнього та великого масштабу.

Звіт з кваліфікаційної роботи виконано згідно матеріалів [1-4]. Результати роботи пройшли апробацію на одинадцятій міжнародній науково-практичній конференції «GLOBAL SCIENCE: PROSPECTS AND INNOVATIONS».

Отримані результати дослідження можна віднести до Цілей сталого розвитку 8 «Гідна праця та економічне зростання», а саме до пункту 8.2: «Підвищувати ефективність виробництва на засадах сталого розвитку та розвитку високотехнологічних конкурентних виробництв». Успішна реалізація запропонованих рішень сприятиме створенню стійких і конкурентоспроможних виробничих систем.

1 АНАЛІЗ СУЧАСНИХ СИСТЕМ МОНІТОРИНГУ ТЕХНОЛОГІЧНИХ ПРОЦЕСІВ

1.1 Моніторингова складова автоматизованої системи

Моніторингова складова автоматизованої системи є ключовим елементом сучасного виробництва, що забезпечує не лише безперервність процесів, але й їх оптимізацію, підвищення ефективності та точності роботи. Її функціонування базується на інтеграції різноманітних інструментів і технологій, які дозволяють автоматизувати процеси збору, аналізу та інтерпретації даних у реальному часі.

Одним із фундаментальних компонентів є технології Інтернету речей (IoT), які об'єднують різноманітні сенсори, контролери й інші пристрої у єдину мережу для забезпечення всебічного моніторингу процесів [5]. Використання розподілених сенсорних мереж дозволяє здійснювати моніторинг навіть у найвіддаленіших ділянках виробництва, а передача даних у хмарні системи забезпечує централізовану обробку та аналіз. Завдяки цьому можна відслідковувати стан обладнання, оперативно виявляти аномалії або відхилення від нормальних параметрів, мінімізуючи ризики аварій та простоїв.

Системи на кшталт SCADA (Supervisory Control and Data Acquisition) є прикладом інтегрованих рішень, що дозволяють здійснювати як моніторинг, так і оперативне управління виробничими процесами [6]. SCADA забезпечує можливість одночасного моніторингу тисяч змінних і візуалізації даних через зручні інтерфейси, що полегшує прийняття рішень на основі реального стану системи. Це особливо важливо для складних виробничих ліній, де кожен параметр може впливати на загальну ефективність роботи.

Інтеграція IoT-пристроїв із хмарними платформами, такими як Azure IoT Hub, надає виробничим компаніям нові можливості для масштабування й оптимізації своїх операцій. Завдяки сенсорам, розташованим у критично важливих точках виробничого процесу, здійснюється безперервний збір даних, таких як

температурні, вібраційні або тискові показники. Azure IoT Hub забезпечує безпечну передачу цих даних у хмару, де вони можуть бути збережені, оброблені й використані для аналітики. Це відкриває шлях до створення прогнозних моделей, які дозволяють оцінити ймовірність виникнення збоїв ще до їхнього фактичного настання.

Хмарні технології в цьому контексті забезпечують надзвичайну гнучкість і економічну ефективність. Системи можуть бути масштабовані відповідно до зростаючих вимог бізнесу, що дозволяє підприємствам адаптувати свої ресурси до конкретних потреб без зупинки виробництва. Крім того, хмарні рішення забезпечують високу швидкість доступу до оброблених даних і дають змогу здійснювати аналіз у реальному часі, що підвищує оперативність прийняття управлінських рішень.

Ключовим аспектом моніторингових систем є їх роль у забезпеченні сталого розвитку промисловості. Постійний моніторинг сприяє підтримці високого рівня продуктивності, знижує витрати на технічне обслуговування завдяки ранньому виявленню потенційних несправностей і сприяє зменшенню впливу на навколишнє середовище. Наприклад, використання сенсорів для моніторингу витоків у трубопроводах допомагає не лише знизити втрати ресурсів, але й мінімізувати шкоду екології.

Застосування аналітичних алгоритмів у моніторингових системах додає їм додаткової цінності. Такі алгоритми дозволяють не лише відстежувати поточний стан процесів, але й прогнозувати майбутні зміни, що дає змогу запобігати критичним відмовам у роботі обладнання. Наприклад, прогнозування на основі даних про вібрацію може дозволити своєчасно ідентифікувати зношення підшипників, що дає змогу замінити їх до моменту виходу з ладу.

Таким чином, моніторингова складова автоматизованих систем виконує не лише роль інструменту контролю, але й є ключовим фактором для прийняття стратегічних управлінських рішень. Вона сприяє підвищенню ефективності роботи підприємств, зниженню операційних витрат, а також створенню умов для сталого розвитку та впровадження інноваційних рішень.

1.2 Види та категорії систем моніторингу

Сучасна класифікація систем моніторингу технологічних процесів є досить різноманітною, а і її структура базується на таких критеріях, як рівень автоматизації, тип контрольованих параметрів, сфера застосування, спосіб отримання даних, принцип роботи тощо.

За рівнем автоматизації розрізняють ручні та автоматизовані системи моніторингу. Ручні системи потребують безпосередньої участі оператора для збору, обробки та аналізу даних, що є менш ефективним підходом через часові затримки між отриманням інформації та реагуванням на відхилення від норми. Автоматизовані системи, навпаки, функціонують автономно, забезпечуючи збір даних у режимі реального часу, їх миттєвий аналіз та виявлення можливих проблемних місць є беззаперечною перевагою. Такий підхід є більш ефективним у промисловому середовищі, оскільки він дозволяє мінімізувати вплив людського фактору та знижує ймовірність виникнення критичних помилок.

За типом контрольованих параметрів виділяють системи моніторингу фізичних, хімічних та енергетичних показників [7]. Фізичні системи зосереджені на контролі параметрів, таких як температура, тиск, рівень шуму та вібрації, що важливо для забезпечення належного стану обладнання. Хімічні системи відповідають за вимірювання концентрації певних речовин, рівня pH та вмісту кисню, що є критичним у хімічній та фармацевтичній галузях. Енергетичні системи спрямовані на контроль ефективності споживання енергії та сприяють зменшенню втрат, що важливо для енергоємних підприємств.

За способом отримання даних системи моніторингу поділяються на локальні та дистанційні. Локальні системи збирають інформацію безпосередньо на місці проведення процесу, що забезпечує оперативність, проте обмежує доступність даних виключно межами підприємства. Дистанційні системи, натомість, дозволяють передавати зібрану інформацію до віддалених центрів обробки, що підвищує гнучкість у прийнятті рішень і забезпечує доступ до даних у масштабах всієї компанії.

Залежно від принципу роботи виділяють аналогові та цифрові системи моніторингу. Аналогові системи базуються на використанні аналогових сенсорів та механізмів передачі сигналів і мають обмежену точність порівняно з цифровими, які застосовують інтелектуальні алгоритми та цифрові сенсори для збору й аналізу даних. Завдяки цифровим технологіям сучасні системи моніторингу здатні забезпечувати високий рівень точності та швидкості обробки інформації, що є надзвичайно важливим у промисловості.

Такий комплексний підхід до класифікації систем моніторингу дозволяє підібрати оптимальне рішення для кожного конкретного виробничого процесу, враховуючи його унікальні особливості та вимоги.

1.3 Переваги та недоліки існуючих рішень

Моніторинг промислових процесів надає компаніям суттєві переваги, дозволяючи досягти високої ефективності та конкурентоспроможності за рахунок більш глибокого розуміння функціонування виробничих систем. Завдяки моніторингу підприємства отримують змогу систематично відстежувати критичні параметри технологічних процесів, визначати вузькі місця в операціях і вчасно реагувати на будь-які відхилення. Це дозволяє не лише уникати значних фінансових втрат, але й забезпечує стабільність виробничих процесів у довгостроковій перспективі. Однією з ключових переваг є можливість виявляти проблеми на ранніх етапах, що суттєво знижує ризики аварій та простоїв обладнання, сприяючи мінімізації непередбачуваних витрат.

Сучасні автоматизовані системи моніторингу забезпечують оперативний збір, обробку та аналіз даних у режимі реального часу. Це стає можливим завдяки використанню IoT-пристроїв, які встановлюються у критично важливих точках виробничих ліній. Дані, отримані з таких сенсорів, передаються до централізованих платформ, наприклад, таких як Azure IoT Hub, де вони обробляються аналітичними алгоритмами для подальшого використання у прийнятті управлінських рішень. Автоматизація цього процесу дозволяє мінімізувати участь людини та уникнути

можливих помилок, спричинених людським фактором, тим самим підвищуючи ефективність системи.

Крім того, сучасні рішення з моніторингу дозволяють значно оптимізувати виробничі цикли, зменшуючи час простою обладнання та підвищуючи загальну продуктивність [8]. Оптимізація виробничих процесів безпосередньо впливає на зниження енергоспоживання та витрат на технічне обслуговування, що є важливим фактором для підприємств з високими витратами ресурсів. Використання аналітичних алгоритмів дозволяє здійснювати прогнозування відмов обладнання, що сприяє запобіганню аварійних ситуацій та забезпечує безперервність виробництва.

Водночас важливим аспектом є питання кібербезпеки, яке потребує все більшої уваги в умовах активного розвитку IoT та хмарних технологій. Сучасні моніторингові системи значною мірою базуються на зборі даних з IoT-пристроїв, що створює ризики несанкціонованого доступу до цих даних або їхньої модифікації. Наприклад, у разі кіберзлочинної діяльності, яка спрямована на отримання доступу до даних сенсорів або централізованих платформ, можуть виникати серйозні загрози для стабільності виробничих процесів. З метою забезпечення безпеки необхідно впроваджувати комплексні рішення, що включають шифрування даних, багатофакторну автентифікацію та регулярний аудит системи на предмет вразливостей. Також важливим є використання захищених протоколів передачі даних, таких як TLS, що запобігає можливим перехопленням інформації під час її передачі. Принцип роботи протоколу TLS наведено на рис. 1.1.

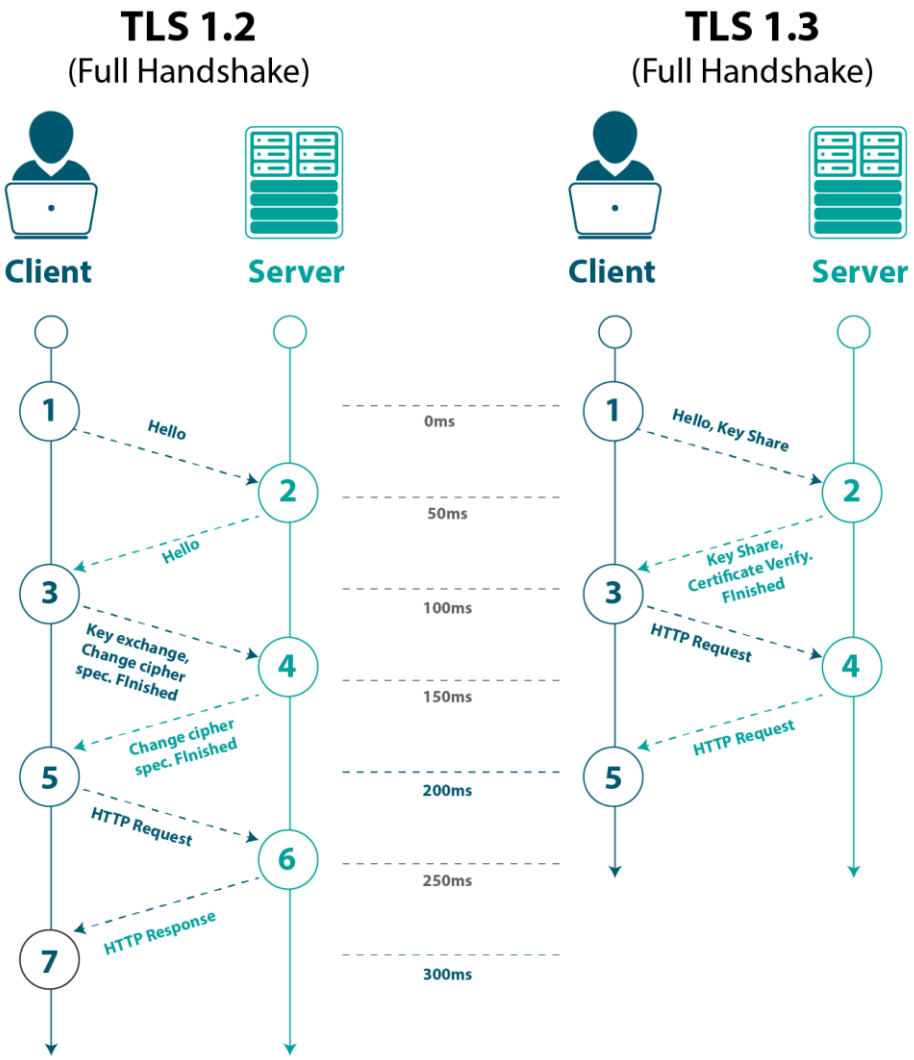

Рисунок 1.1– Принцип роботи протоколу TLS

Ще одним перспективним напрямом розвитку є впровадження новітніх технологій, таких як блокчейн, для забезпечення прозорості та захисту даних, зібраних моніторинговими системами. Блокчейн дозволяє створювати децентралізовану базу даних, яка захищена від несанкціонованого доступу та змін, тим самим підвищуючи надійність і довіру до системи. Наприклад, використання блокчейну може бути особливо корисним для верифікації даних, отриманих з IoT-сенсорів, що забезпечує їхню автентичність і цілісність.

Серед новітніх розробок у сфері моніторингу також заслуговують на увагу інтеграція таких систем із роботизованими платформами. Роботизовані системи

дозволяють автоматизувати не лише моніторинг, але й діагностику, а також безпосереднє втручання у виробничі процеси у разі виникнення відхилень. Наприклад, автономні роботи можуть бути запрограмовані для виконання діагностичних завдань, таких як перевірка технічного стану обладнання або виявлення аномалій у виробничих лініях. Це не лише підвищує швидкість реагування, але й забезпечує більш високу точність у порівнянні з традиційними методами моніторингу.

Однак, незважаючи на значні переваги, системи моніторингу мають і певні недоліки, які варто враховувати під час впровадження. Основним викликом є висока вартість таких систем, яка може стати бар'єром для підприємств малого та середнього бізнесу. Інтеграція моніторингових рішень в існуючі виробничі процеси потребує значних інвестицій, а також витрат часу та ресурсів на навчання персоналу та налаштування обладнання. Крім того, важливо враховувати складність адаптації таких систем до швидко змінюваних умов ринку, що може потребувати додаткових витрат на модернізацію обладнання чи програмного забезпечення.

Отже, моніторинг є важливим інструментом для підвищення ефективності, продуктивності та безпеки виробничих процесів. Завдяки сучасним технологіям, таким як IoT, блокчейн і роботизовані платформи, моніторингові системи мають значний потенціал для оптимізації витрат, забезпечення кібербезпеки та створення умов для сталого розвитку підприємств. Інтеграція таких систем є стратегічним кроком для будь-якої компанії, яка прагне посилити свою конкурентоспроможність та адаптуватися до сучасних викликів.

1.4 Застосування моніторингу в різних галузях промисловості

Автоматизовані системи моніторингу є невід'ємною складовою різних галузей промисловості завдяки їхній гнучкості, високій ефективності та здатності до адаптації під специфічні виробничі потреби [9]. У нафтогазовій галузі моніторинг відіграє критичну роль, особливо при експлуатації нафтових

свердловин, де необхідно забезпечити стабільну роботу обладнання в умовах складного середовища. Системи моніторингу контролюють стан насосів, трубопроводів та інших компонентів, що дозволяє своєчасно виявляти потенційні несправності та уникати можливих аварій, які можуть призвести до значних фінансових втрат. Крім того, автоматизовані системи здійснюють постійний контроль викидів у навколишнє середовище, що сприяє зменшенню шкідливого впливу на екологію та допомагає компаніям дотримуватися суворих екологічних стандартів. Завдяки цим системам підприємства можуть не лише підвищити ефективність своєї роботи, а й зменшити витрати на ремонт обладнання, вчасно запобігаючи можливим несправностям.

В енергетичній галузі автоматизовані системи моніторингу застосовуються для контролю параметрів електромереж, таких як напруга, частота та рівень енергоспоживання. Це дозволяє не тільки швидко виявляти відхилення від стандартних параметрів, але й своєчасно запобігати перевантаженням мереж, які можуть призвести до перебоїв у постачанні енергії. Наприклад, моніторинг стану енергетичного обладнання, такого як турбіни й генератори, дозволяє оптимізувати процес виробництва електроенергії, забезпечуючи його безперервність. Ці системи також сприяють ефективному управлінню ресурсами, дозволяючи зменшувати енерговитрати шляхом аналізу даних про споживання енергії в реальному часі та рекомендацій щодо оптимізації процесів. Зниження енергетичних витрат є важливим економічним чинником, який підвищує конкурентоспроможність підприємств у довгостроковій перспективі.

У хімічній промисловості автоматизовані системи моніторингу є критично важливими, оскільки забезпечують постійний контроль таких параметрів, як температура, тиск та інші ключові характеристики, від яких залежить безпека і стабільність хімічних реакцій. Це мінімізує ризик аварійних ситуацій, які можуть мати катастрофічні наслідки для здоров’я працівників та навколишнього середовища. Завдяки високій точності вимірювань ці системи дозволяють виявляти навіть найменші відхилення від норми, наприклад, витоки небезпечних речовин, що значно знижує ризик виникнення катастроф. Крім того, автоматизовані системи

моніторингу сприяють підвищенню ефективності роботи обладнання та зниженню витрат на технічне обслуговування, оскільки своєчасний контроль дозволяє уникнути незапланованих простоїв.

У військовій промисловості автоматизовані системи моніторингу забезпечують контроль за технічним станом бойової техніки, що особливо важливо для підтримки її готовності до оперативного використання. Реалізація таких систем дозволяє швидко реагувати на потенційні несправності або збої, що є критичним фактором у забезпеченні обороноздатності країни. Постійний моніторинг стану озброєння сприяє підвищенню ефективності управління ресурсами та дозволяє значно зменшити витрати на технічне обслуговування.

Окрім практичного застосування у галузях, автоматизовані системи моніторингу також демонструють високу економічну доцільність. Інвестиції у впровадження таких систем окупаються завдяки суттєвому зниженню витрат на технічне обслуговування, ремонт обладнання та енергоспоживання. Наприклад, використання превентивного обслуговування, заснованого на даних моніторингу, дозволяє уникати раптових зупинок, що значно зменшує витрати підприємств на аварійні ремонти. Автоматизовані системи також дають змогу оптимізувати виробничі процеси, підвищуючи продуктивність та рентабельність. Зокрема, завдяки масштабованості рішень, підприємства можуть адаптувати системи моніторингу до змін у своїй діяльності, зберігаючи при цьому високу ефективність роботи.

Таким чином, автоматизовані системи моніторингу є невід'ємною частиною сучасної промисловості, забезпечуючи надійність, ефективність та безпеку технологічних процесів. Їхнє впровадження дозволяє знижувати витрати, підвищувати якість продукції та адаптуватися до швидкозмінних ринкових умов, що є ключовими факторами для успішного розвитку підприємств.

1.5 Висновки до першого розділу

У цьому розділі були досліджені основні аспекти моніторингу в автоматизованих системах технологічних процесів. Моніторингова складова є надзвичайно важливою для забезпечення ефективного, безпечного та стабільного функціонування виробничих процесів. Застосування таких систем дозволяє підприємствам оперативно виявляти відхилення від нормального режиму роботи, мінімізувати ризики аварійних ситуацій та значно знизити витрати на ремонт і технічне обслуговування обладнання. У сучасних умовах автоматизація цих процесів забезпечує безперервний контроль за критичними параметрами, що є особливо важливим у сферах з підвищеним рівнем відповідальності, таких як енергетика, хімічна та військова промисловості [10].

Проаналізовані види систем моніторингу дозволили визначити різні підходи до їх класифікації, зокрема за рівнем автоматизації, типом контрольованих параметрів, сферою застосування, способом отримання даних та принципом роботи. Така різноманітність класифікацій дозволяє гнучко адаптувати моніторингові системи до конкретних потреб підприємства, забезпечуючи максимальну ефективність та надійність.

Вивчення переваг та недоліків існуючих рішень показало, що автоматизовані системи моніторингу мають значний потенціал для оптимізації виробничих процесів та забезпечення дотримання екологічних і безпекових стандартів. У різних галузях промисловості такі системи використовуються для контролю технічного стану обладнання, оптимізації енергоспоживання, виявлення витоків небезпечних речовин та дотримання стандартів якості продукції.

2 ПРОЄКТУВАННЯ СТРУКТУРИ ТА РОЗРОБКА АВТОМАТИЗОВАНОЇ СИСТЕМИ МОНІТОРИНГУ

2.1 Аналіз вимог до системи моніторингу

Основна вимога до системи моніторингу полягає у здатності до безперервного збору даних у реальному часі. Це потребує ефективного механізму обробки та зберігання інформації з мінімальною затримкою, що дозволяє контролювати параметри технологічних процесів майже миттєво. Наприклад, для технологічного обладнання, що працює в умовах високої температури або підвищеного тиску, затримка у відображенні даних може призвести до аварійних ситуацій, що негативно вплине на безпеку та ефективність роботи виробництва.

Крім швидкодії, однією з найважливіших вимог є масштабованість системи, що передбачає можливість обробляти зростаючі обсяги даних і адаптуватися до розширення виробництва без значних перебудов. У контексті хмарних рішень це досягається завдяки використанню таких інструментів, як Azure Queue Bus та IoT Hub, які дозволяють обробляти дані від великої кількості сенсорів та пристроїв у розподілених середовищах [11]. На рис. 2.1 зображено принцип дії Azure IoT Hub.

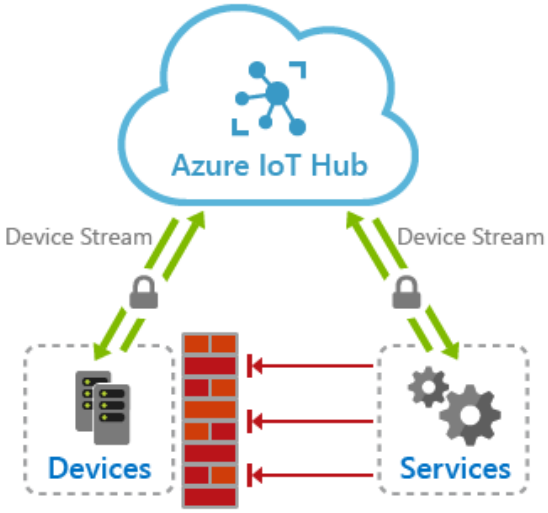

Рисунок 2.1 – Принцип дії Azure IoT Hub

Цей підхід забезпечує не лише простоту масштабування, а й підвищену стійкість системи до навантаження, що є ключовим для надійного функціонування системи в умовах пікового завантаження.

Запорука успішного процесу моніторингу та прогнозування є визначення ключових показників ефективності (Key Performance Indicators, KPI), на основі яких буде здійснюватися оцінка стану процесів. До таких показників можуть належати рівень енергоспоживання, температура, швидкість потоку, тиск, рівень вібрації тощо, залежно від конкретних виробничих потреб. Виявлення критичних параметрів дозволяє забезпечити цільовий контроль і запобігти можливим відхиленням, використовуючи налаштування тригерів і сповіщень, які допомагають миттєво реагувати на небезпечні зміни.

2.2 Архітектура рішення на базі Azure

Архітектура автоматизованої системи моніторингу, побудованої на базі хмарної платформи Azure, забезпечує комплексне рішення для безперервного збору, обробки, зберігання та аналізу даних, а також сповіщення користувачів про критичні ситуації в реальному часі [12]. У цій системі інтегруються різні компоненти, що взаємодіють між собою для досягнення оптимальної точності та швидкості виявлення аномалій.

Система починається з датчиків, встановлених на об'єктах моніторингу, які здійснюють безперервне вимірювання показників таких, як температура, тиск, рівень вологості, швидкість потоку чи вібрація. Ці датчики збирають дані у режимі реального часу і відправляють їх до хмарної платформи через Azure Device Provisioning Service (DPS). На рис. 2.2 зображено принцип дії Device Provisioning Service.

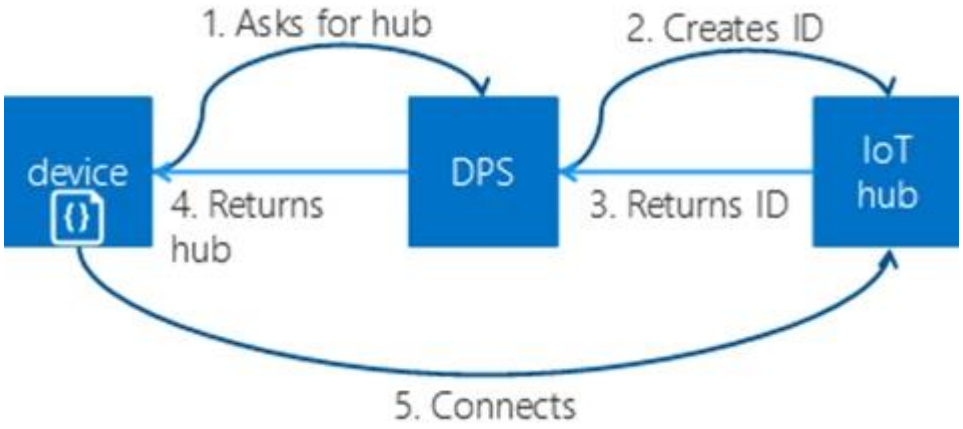

Рисунок 2.2 – Принцип дії Device Provisioning Service

Azure DPS виконує функцію централізованої служби для автоматичного додавання нових пристроїв у мережу, спрощуючи управління підключенням нових точок моніторингу [13]. Завдяки DPS будь-який новий пристрій, підключений до системи, автоматично отримує всі необхідні конфігурації для з'єднання з основним шлюзом – Azure IoT Hub, що суттєво знижує час і витрати на налаштування обладнання.

Azure IoT Hub виступає основним комунікаційним центром для всіх підключених пристроїв. Він забезпечує двосторонню передачу даних між пристроями та хмарною інфраструктурою, дозволяючи не лише отримувати дані з датчиків, але й надсилати команди зворотного зв'язку. IoT Hub підтримує великий обсяг одночасних підключень і дає змогу масштабувати систему відповідно до потреб користувача. Вся отримана інформація з IoT Hub розподіляється на кілька потоків для подальшої обробки та аналізу.

Azure Stream Analytics, інтегрований з IoT Hub, забезпечує обробку даних у реальному часі. За допомогою Stream Analytics jobs інформація розподіляється в три окремі потоки. На рис. 2.3 зображено принцип дії Stream Analytics.

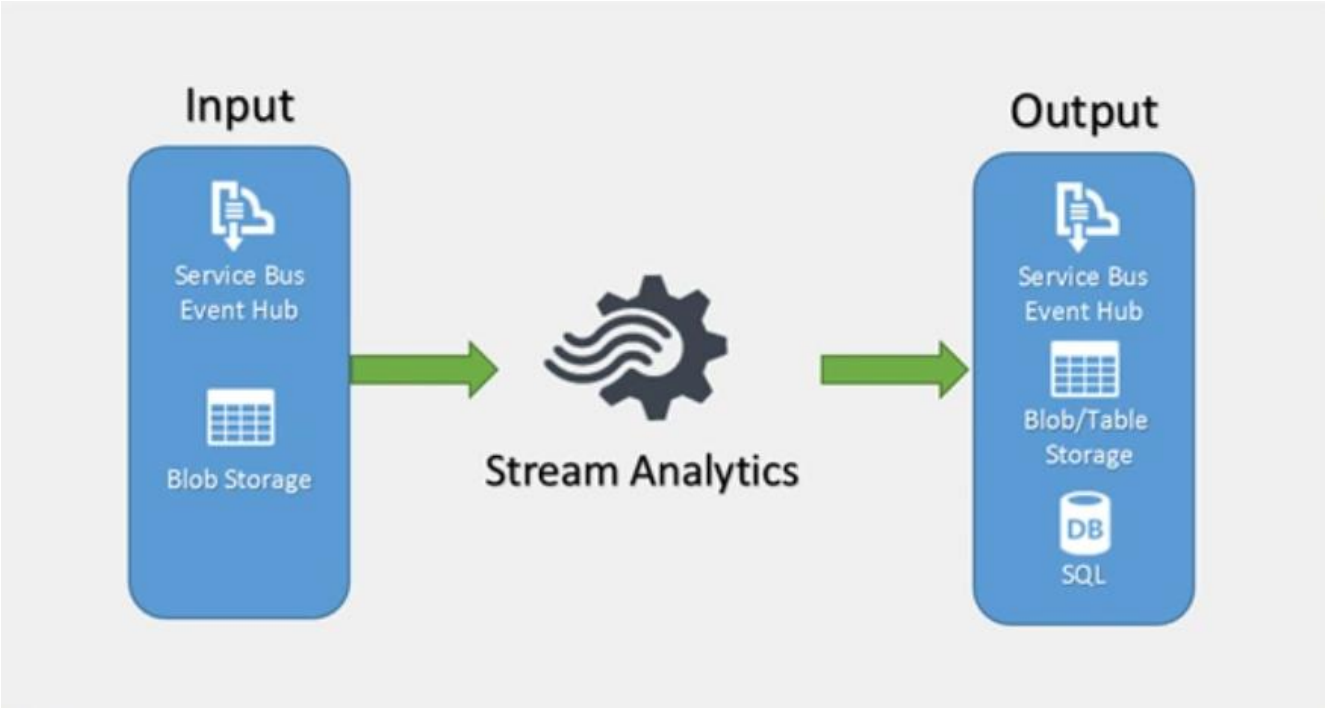

Рисунок 2.3 – Принцип дії Stream Analytics Job

Перший потік даних направляється до Power BI, платформи бізнес-аналітики, де дані обробляються та візуалізуються у вигляді інтерактивних дашбордів і звітів. Це дозволяє операторам та керівництву отримувати актуальну інформацію про стан об'єктів моніторингу, а також аналізувати тенденції для прийняття обґрунтованих рішень. Дашборди в Power BI налаштовуються під індивідуальні потреби компанії, що робить їх гнучким інструментом для моніторингу ефективності процесів.

Другий потік, оброблений Azure Stream Analytics, перенаправляється в Azure Blob Storage, де дані зберігаються для довгострокового архівування. Використання Blob Storage дозволяє надійно зберігати великі обсяги інформації з доступом для подальшого аналізу або створення звітів на історичних даних.

Довготривале зберігання даних є важливим елементом для виявлення закономірностей, ретроспективного аналізу та звітності. Це дає можливість оцінювати ефективність обладнання протягом тривалих періодів та прогнозувати його можливі несправності на основі попередніх даних.

Третій потік Stream Analytics направляє оброблені та агреговані дані в BusQueue, який використовується для аналізу аномалій.

BusQueue забезпечує механізм асинхронної передачі повідомлень між різними компонентами системи, що уможливлює незалежне масштабування та підвищує надійність обробки даних. Принцип його роботи полягає у тому, що Stream Analytics, виконавши початкову обробку та агрегацію даних, відправляє сформовані повідомлення до черги, де вони тимчасово зберігаються до моменту споживання призначеним сервісом. Це означає, що процес надсилання і процес обробки повідомлень відбуваються незалежно один від одного: надсилаючий додаток не чекає на завершення обробки, а цільовий сервіс отримує повідомлення у зручний для нього момент. Така архітектурна схема усуває ризик одночасного навантаження на приймаючий додаток і дозволяє працювати з нерівномірним потоком даних. Водночас кожне повідомлення, що надходить до BusQueue, може містити сукупність показників, згенерованих з різних джерел, що забезпечує повноту вхідних даних для подальшого аналізу аномалій. Такий підхід є надзвичайно гнучким при розподіленій архітектурі: у разі зростання обсягів даних можна збільшити кількість споживачів черги, що підвищує пропускну здатність системи й забезпечує мінімізацію затримок під час аналізу аномальних подій.

Принцип дії BusQueue наведено на рис. 2.4.

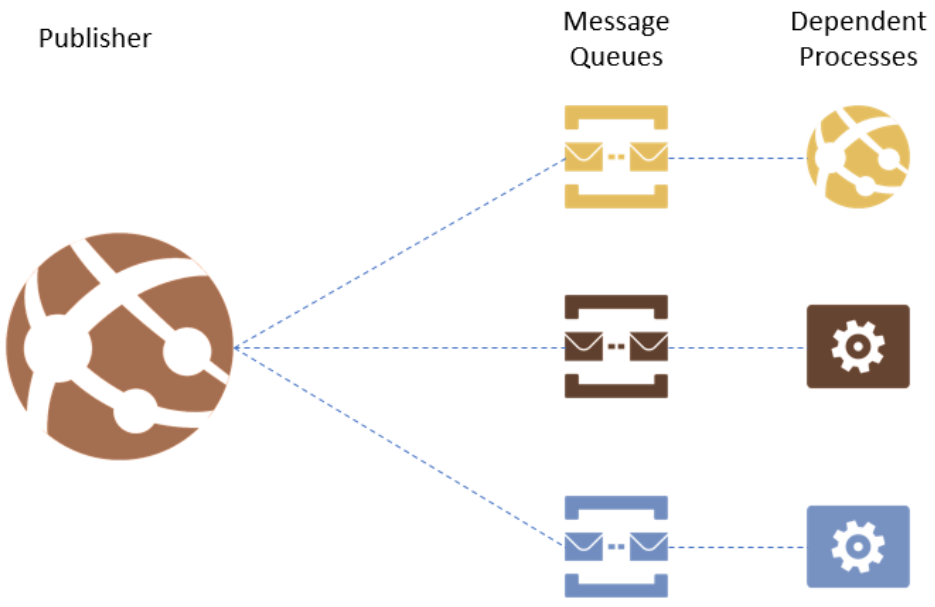

Рисунок 2.4 – Принцип дії BusQueue

В разі виявлення критичних ситуацій, таких як вихід параметрів за допустимі межі, що відбувається ще на етапі агрегування даних у Stream Analytic Job, запускається автоматизований сценарій реагування за допомогою виклику Logic App повідомленням з QueueBus. LogicApp у свою чергу надсилає сповіщення на пошту відповідальному персоналу, повідомляючи про необхідність оперативного втручання. Оповіщення може бути налаштоване як SMS, електронний лист або повідомлення у корпоративній системі обміну повідомленнями, що дозволяє швидко реагувати на потенційні проблеми та зменшити ризики пошкоджень обладнання. На рис. 2.5 зображено принцип дії Logic App.

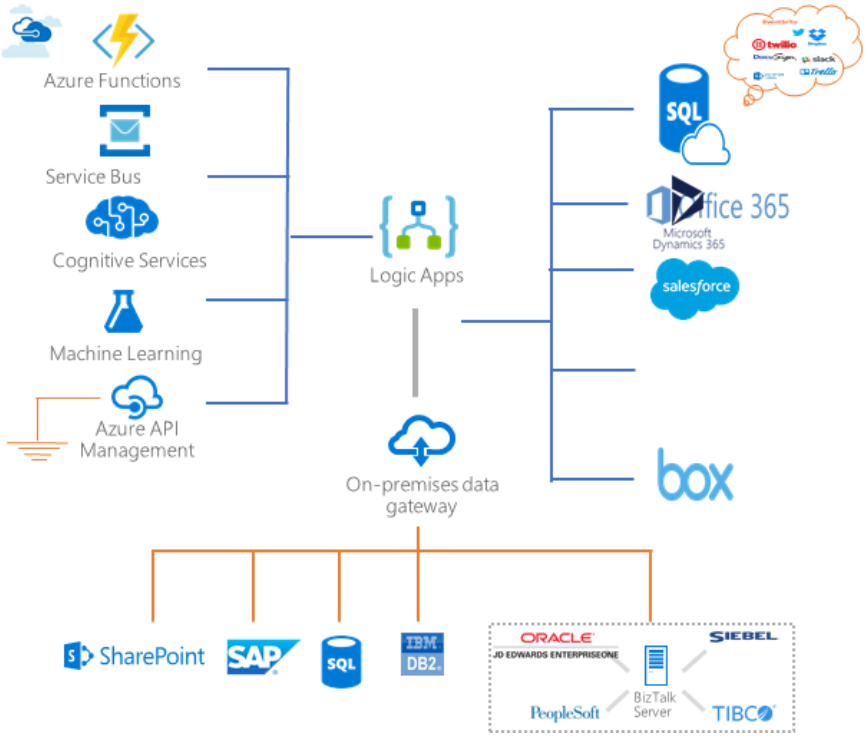

Рисунок 2.5 – Принцип дії Logic App

Поєднання таких компонентів, як IOTHub, BusQueue, Stream Analytics Job, Power BI, Blob Storage, Logic App, створює єдину інтегровану екосистему для моніторингу та оповіщення. Взаємодія між компонентами є автоматизованою, що дає змогу уникнути ручного втручання в процеси моніторингу та забезпечує високу швидкість і точність виявлення аномалій. Цей підхід дозволяє компаніям суттєво

підвищити ефективність контролю за станом обладнання, що особливо важливо в умовах масштабних промислових операцій.

Важливим аспектом архітектури є її масштабованість. Завдяки Azure платформа може обробляти як невеликі обсяги даних, так і дані від тисяч пристроїв одночасно, що дозволяє адаптувати рішення під різні масштаби виробничих і промислових підприємств. Всі складові рішення інтегруються через єдину інфраструктуру, що спрощує управління і налаштування, а також знижує витрати на впровадження та підтримку.

Таким чином, архітектура на базі Azure надає універсальне рішення для моніторингу технологічних процесів з розширеними можливостями для аналізу даних, оповіщення про критичні події та довготривалого зберігання інформації [14]. Це робить її ефективним інструментом для контролю за станом технологічних об’єктів, забезпечуючи надійність і безперервність виробничих процесів. На рис. 2.6 зображено кінцевий вигляд архітектури на базі Azure.

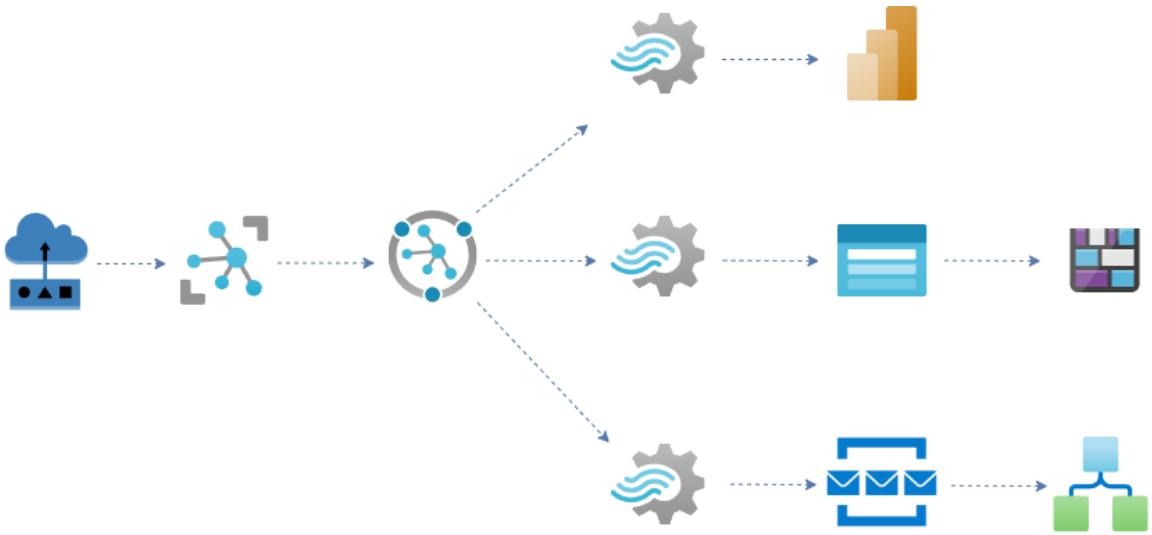

Рисунок 2.6 – Архітектура на базі Azure

2.3 Застосування теорії автоматичного управління в системах моніторингу

Теорія автоматичного управління (ТАУ) є базовою науковою дисципліною, яка широко використовується при розробці автоматизованих систем моніторингу

та управління технологічними процесами [15-16]. Її важливість полягає у забезпеченні стабільності, точності та адаптивності роботи таких систем. ТАУ формує теоретичну основу для аналізу динамічних систем, створення алгоритмів управління та підвищення ефективності технологічних процесів.

Одним із ключових аспектів ТАУ є використання математичних моделей для опису динаміки об'єктів. Моделі, побудовані на основі передаточних функцій, рівнянь стану або інших математичних підходів, дозволяють описати поведінку технологічних процесів у різних умовах. Це є важливим для моніторингу, оскільки такі моделі можуть слугувати базою для прогнозування аномалій і визначення меж стабільної роботи системи.

Зворотній зв'язок є центральним елементом у застосуванні ТАУ до систем моніторингу. Завдяки ньому забезпечується постійна корекція параметрів роботи системи на основі отриманих даних. У теоретичному контексті це дозволяє мінімізувати похибки та підвищити надійність процесу. У практичному аспекті це може бути реалізовано через адаптивні алгоритми, які автоматично коригують налаштування залежно від змін у зовнішньому середовищі

Потенційні напрямки застосування ТАУ в автоматизованих системах моніторингу включають впровадження PID-регуляторів, які дозволяють підтримувати ключові параметри процесів у стабільному стані [17]. Це може бути особливо корисним для стабілізації роботи сенсорів або забезпечення постійного рівня якості даних, які передаються до хмарної платформи.

Крім того, принципи ТАУ можуть бути застосовані для покращення механізмів прогнозування. Спостерігачі стану, які використовуються для оцінки невимірюваних параметрів, можуть стати ефективним інструментом для передбачення потенційних збоїв у системі та попередження аварійних ситуацій.

Таким чином, теорія автоматичного управління є фундаментальним підходом для побудови систем моніторингу. Інтеграція її принципів у сучасні рішення дозволяє значно розширити функціональні можливості системи, забезпечивши її надійність, стабільність та адаптивність до змін у виробничих процесах.

2.4 Висновки до другого розділу

У межах розробленої архітектури на базі Azure було враховано основні вимоги до системи моніторингу, що передбачають безперервний збір та обробку даних у реальному часі, гнучке масштабування, а також надійне довготривале зберігання інформації для подальшого аналізу. У ході проєктування було акцентовано увагу на можливості швидкої реакції на зміну критичних параметрів шляхом інтеграції Stream Analytics, що виконує оперативну обробку даних і виявлення аномалій, з BusQueue, який забезпечує асинхронну передачу повідомлень між компонентами системи. Поєднання в одному рішенні IoT Hub, служби Device Provisioning Service, BusQueue, хмарного сховища Blob Storage, а також аналітичних можливостей Power BI та інструментів Logic App дозволило сформувати єдине середовище для масштабованого та оперативного збору, аналізу та візуалізації показників технологічних процесів, а також для своєчасного оповіщення про відхилення [18]. Система продемонструвала високу адаптивність до змінних навантажень за рахунок хмарних сервісів, що легко масштабуються, і дає змогу автоматично підключати нові пристрої без складних процедур налаштування. Реалізований принцип трьох потоків даних забезпечує розподіл інформації за пріоритетами та сценаріями використання: онлайн-відображення ключових показників у Power BI, довготривале архівування в Blob Storage та поглиблений аналіз аномалій через BusQueue. Такий підхід дає змогу ефективно керувати як поточним контролем виробничих процесів, так і їхньою ретроспективною оцінкою, що є критично важливим для виявлення тенденцій, оцінювання ресурсних витрат і прогнозування можливих збоїв. У підсумку сформована надійна, масштабована та гнучка система, яка відповідає потребам сучасної промисловості та сприяє досягненню підвищеного рівня безпеки й економічної ефективності виробництва за рахунок оперативного реагування на критичні події та надання аналітичної інформації для ухвалення виважених управлінських рішень.

3 РОЗРОБЛЕННЯ СИМУЛЯТОРА СЕНСОРНИХ ДАНИХ ДЛЯ МОНІТОРИНГУ ТЕХНОЛОГІЧНИХ ПРОЦЕСІВ

3.1 Структура симулятора

Симулятор сенсорних даних розроблено з урахуванням задач моніторингу та прогнозування стану технологічних процесів. Основною його складовою є головний інтерфейс, який слугує для інтерактивної взаємодії користувача із системою. Інтерфейс дозволяє реєструвати та підключати сенсори, спостерігати за їхнім статусом. Приклад інтерфейсу наведено на рис. 3.1.

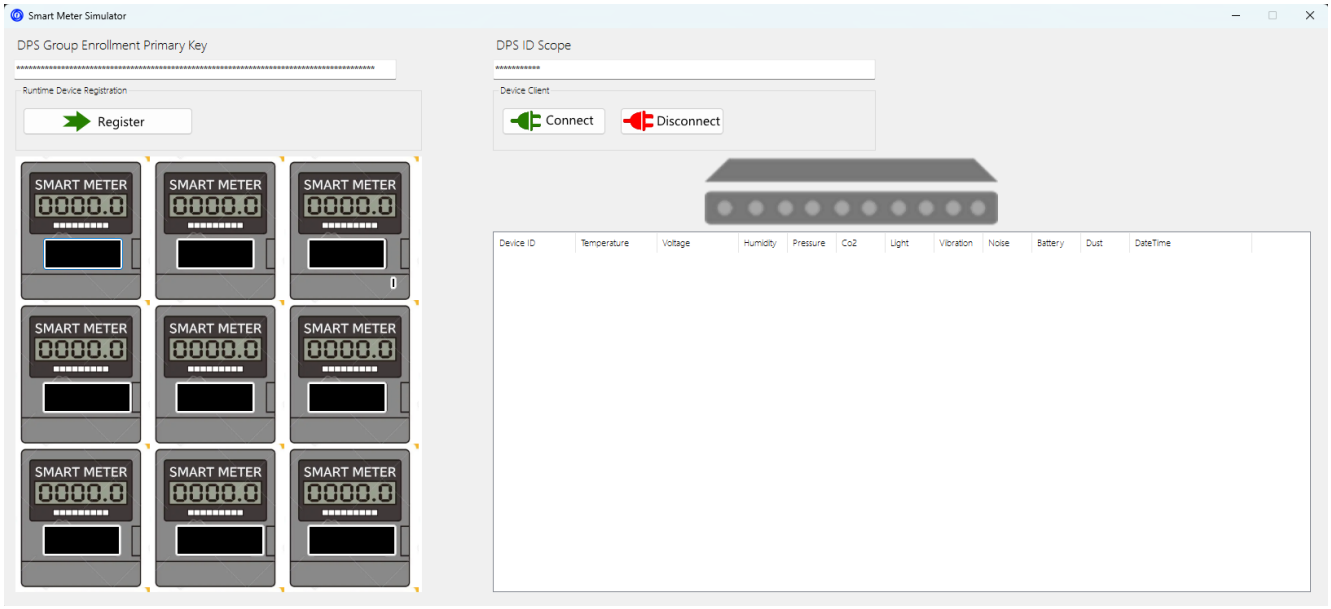

Рисунок 3.1 – Інтерфейс симулятора сенсорних даних

Ключовим елементом симулятора є клас Sensor, який відповідає за генерацію та імітацію показників сенсорів. Кожному з цих сенсорів було надано для показовості по десять параметрів одночасно, таких, як температура, напруга, вологість, тиск, рівень вуглекислого газу (CO2), освітленість, вібрація, шум, заряд батареї та рівень пилу. Для кожного з цих показників реалізовано алгоритми створення аномалій, що враховують випадкові імовірності та дозволяють

моделювати реальні умови роботи технологічного обладнання. Для передачі даних між сенсорами та хмарними сервісами використовується протокол MQTT [19]. Цей протокол обрано завдяки його здатності забезпечувати надійність передачі, низьку затримку та ефективну взаємодію навіть із великою кількістю пристроїв у масштабованих системах. Принцип роботи протоколу MQTT наведено на рис. 3.2.

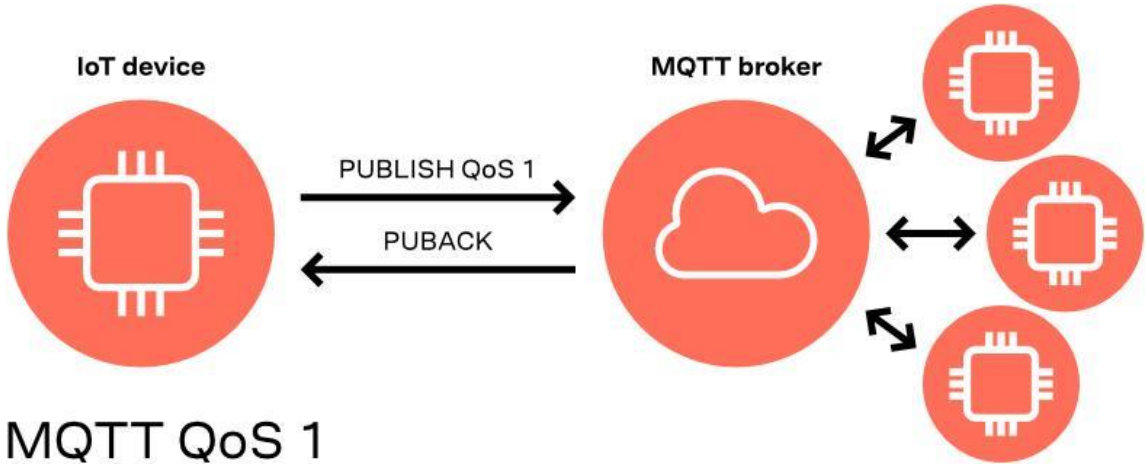

Рисунок 3.2 – Прицнип роботи протоколу MQTT

Процес реєстрації сенсорів реалізовано за допомогою класу DeviceManager, який інтегрується з Azure Device Provisioning Service. Ця функціональність забезпечує безпечне збереження даних та автоматичне призначення унікальних ключів автентифікації для кожного пристрою. Це дає змогу ефективно керувати підключеннями навіть у масштабованих системах із великою кількістю сенсорів.

Для синхронізації роботи сенсорів використовується черга завдань, реалізована в класі BackgroundQueue. Ця система дозволяє обробляти дані у паралельному режимі, забезпечуючи стабільну та безперебійну роботу симулятора. Вона організовує виконання задач, таких як збір, передача та обробка телеметрії, у чітко визначеному порядку.

Для зручності аналізу та обробки телеметрії застосовано клас ListViewColumnSorter. Він дозволяє сортувати дані у візуальному інтерфейсі, полегшуючи процес моніторингу та оцінки показників сенсорів. Завдяки цьому користувач може швидко отримати інформацію про роботу кожного пристрою.

Таким чином, структура симулятора забезпечує повний цикл роботи з сенсорними даними – від генерації показників до їхнього відображення, аналізу та обробки. Інтеграція з хмарними сервісами, підтримка паралельної обробки, візуалізації та використання протоколу MQTT робить цю систему універсальним інструментом для моделювання та дослідження технологічних процесів [20].

3.2 Генерація сенсорних даних

Генерація сенсорних даних у симуляторі базується на логіці, яка відтворює реальні умови роботи технологічних процесів. Основний акцент зроблено на створенні показників, які відповідають фізичним параметрам обладнання, таких як температура, напруга, вологість, тиск, рівень CO2, освітленість, вібрація, шум, заряд батареї та рівень пилу. Для кожного з цих параметрів встановлено діапазони нормальних значень, які імітують реальні показники функціонування обладнання.

Приклад згенерованих даних наведено на рис. 3.3.

Device ID	Temperature	Voltage	Humidity	Pressure	Co2	Light	Vibration	Noise	Battery	Dust	DateTime
Device9	57,0	0,051	44,0	711,1	797,3	8932,0	3,3	5,8	13,7	16,8	2025-01-27T14:48:26
Device6	57,0	0,050	1,5	707,3	546,9	2040,2	2,4	89,9	31,3	341,6	2025-01-27T14:48:20
Device1	52,0	0,049	39,6	777,8	604,5	4917,0	3,2	109,4	22,5	126,7	2025-01-27T14:48:19
Device6	52,0	0,049	27,6	772,3	653,2	3021,8	3,2	33,2	65,9	214,1	2025-01-27T14:48:38
Device3	53,0	0,046	31,4	747,7	600,6	8031,0	3,9	18,5	11,2	285,9	2025-01-27T14:48:19
Device3	54,0	0,042	92,6	749,0	689,8	7704,9	2,4	15,1	59,9	201,0	2025-01-27T14:48:28
Device4	61,0	0,040	88,3	762,8	732,6	4206,4	2,1	99,0	95,6	310,2	2025-01-27T14:48:18
Device5	51,0	0,040	97,6	789,5	559,5	4286,7	0,9	15,9	85,3	377,3	2025-01-27T14:48:25
Device1	69,0	0,035	26,7	756,7	542,1	4829,5	2,6	51,7	48,1	136,9	2025-01-27T14:48:37
Device2	54,0	0,034	65,1	741,8	551,1	3895,3	2,3	110,1	83,2	336,5	2025-01-27T14:48:17
Device2	64,0	0,033	32,5	726,8	509,9	5103,3	4,6	12,3	93,2	44,6	2025-01-27T14:48:26
Device8	54,0	0,032	87,6	752,8	2251,4	6286,0	0,2	70,6	76,5	33,4	2025-01-27T14:48:36
Device4	54,0	0,032	20,7	766,5	635,2	557,7	3,2	106,7	35,8	459,5	2025-01-27T14:48:36
Device0	50,0	0,030	4,7	705,3	587,5	1121,9	4,6	100,7	28,0	16,2	2025-01-27T14:48:15
Device5	58,0	0,030	60,3	787,7	766,7	8896,4	0,4	50,4	42,4	63,3	2025-01-27T14:48:16
Device6	68,0	0,029	37,4	719,9	404,4	3812,1	3,6	92,0	94,4	276,4	2025-01-27T14:48:29
Device3	50,0	0,027	97,0	759,4	595,7	8109,0	0,5	75,4	47,3	10,3	2025-01-27T14:48:37
Device1	54,0	0,025	78,8	734,8	716,2	1663,4	0,8	52,0	34,7	307,4	2025-01-27T14:48:28
Device8	57,0	0,024	25,1	744,0	625,3	9778,7	4,7	57,0	42,3	411,6	2025-01-27T14:48:18
Device0	64,0	0,020	68,8	793,8	508,3	1385,5	3,9	23,8	65,5	398,9	2025-01-27T14:48:25
Device0	61,0	0,019	15,8	755,5	640,5	318,9	1,3	72,4	97,6	398,6	2025-01-27T14:48:34
Device9	60,0	0,018	86,9	794,9	729,4	5746,7	3,5	85,3	17,0	114,1	2025-01-27T14:48:17
Device8	65,0	0,018	22,5	704,0	494,9	3173,9	3,6	101,4	40,1	332,5	2025-01-27T14:48:27
Device9	63,0	0,015	43,0	799,5	769,2	4085,9	4,0	37,8	6,3	1064,4	2025-01-27T14:48:35

Рисунок 3.3 – Приклад згенерованих даних

Особливістю алгоритмів генерації є інтеграція механізмів створення аномалій. Наприклад, температура може раптово змінюватися на великі значення

при імовірності 1%, що моделює перегрів пристрою. Вологість, у свою чергу, може перевищувати 120%, створюючи сценарії несправностей у датчику. Аналогічно, для рівня вібрації, шуму та інших показників додано імовірнісні моделі, які генерують аномалії з частотою 0.5-2% залежно від параметра. Це дозволяє тестувати систему на стійкість до непередбачуваних ситуацій [21].

Генерація даних відбувається в асинхронному режимі, забезпечуючи безперервний потік телеметрії до хмарних сервісів для подальшої обробки та аналізу.

3.3 Реєстрація пристроїв

Реєстрація пристроїв у симуляторі здійснюється з використанням класу DeviceManager, який забезпечує інтеграцію з Azure Device Provisioning Service (DPS) [22]. Цей процес включає автоматичне створення унікальних ключів автентифікації для кожного пристрою та їх подальшу реєстрацію в хмарній інфраструктурі. Завдяки цьому забезпечується безпека передачі даних та ідентифікація сенсорів у масштабованих системах.

Для реєстрації використовується алгоритм створення симетричних ключів на основі групового ключа автентифікації та унікального ідентифікатора пристрою. Цей підхід гарантує, що кожен сенсор отримає унікальний ключ, який буде використовуватися для шифрування та підписування переданої телеметрії. Після генерації ключа пристрій реєструється у службі DPS через протокол MQTT, що забезпечує надійний обмін інформацією між пристроєм і хмарою.

Процес реєстрації включає декілька етапів: генерація симетричного ключа, створення клієнта для реєстрації через протокол MQTT, виконання запиту на реєстрацію та отримання результатів, таких як унікальний хост IoT Hub для кожного пристрою. Завдяки цьому кожен сенсор може бути автоматично доданий до системи без ручного налаштування, що значно полегшує масштабування та управління пристроями.

Цей підхід дозволяє забезпечити надійне підключення сенсорів навіть у системах з великою кількістю пристроїв, мінімізуючи можливі затримки та спрощуючи процес інтеграції нових елементів у систему. Таким чином, реєстрація пристроїв у симуляторі є ефективним і безпечним процесом, що відповідає сучасним вимогам до інфраструктури IoT.

3.4 Висновки до третього розділу

У цьому розділі було розглянуто архітектуру та ключові компоненти симулятора сенсорних даних, включаючи структуру інтерфейсу, механізми генерації даних, алгоритми створення аномалій та процес реєстрації пристроїв. Представлений симулятор забезпечує повний цикл роботи з сенсорними даними – від їхньої генерації до передачі, обробки та візуалізації [23].

Інтеграція з хмарними сервісами, такими як Azure Device Provisioning Service, а також використання протоколу MQTT, дозволяють забезпечити безпеку, масштабованість і надійність роботи системи. Завдяки використанню сучасних алгоритмів і технологій симулятор є універсальним інструментом для моделювання та тестування технологічних процесів, що сприяє підвищенню ефективності моніторингу та прогнозування стану обладнання.

4 МЕХАНІЗМИ КЛАСИФІКАЦІЇ ДАНИХ У ХМАРНОМУ СЕРЕДОВИЩІ STREAM ANALYTICS

4.1. Опис вихідних даних і джерел

Основним джерелом даних є потік телеметрії, що надходить від сенсорів у реальному часі. Дані зчитуються з джерела DataFromSensors, яке містить десять основних полів для різних параметрів сенсорів: температура, напруга, вологість, тиск, рівень CO2, освітленість, вібрація, шум, заряд батареї та рівень пилу. Крім того, кожен запис містить ідентифікатор пристрою (id) та часову мітку події (EventEnqueuedUtcTime). Для забезпечення коректної обробки даних виконується приведення типів за допомогою оператора CAST [24]. Це дозволяє трансформувати всі значення у формат FLOAT, що спрощує подальші математичні обчислення.

Приклад SQL-запиту, який реалізує цей етап, виглядає наступним чином:

```
WITH
InitialData AS
(
   SELECT
      CAST(temp      AS FLOAT) AS raw_temp,
      CAST(voltage   AS FLOAT) AS raw_voltage,
      CAST(humidity  AS FLOAT) AS raw_humidity,
      CAST(pressure  AS FLOAT) AS raw_pressure,
      CAST(co2       AS FLOAT) AS raw_co2,
      CAST(light     AS FLOAT) AS raw_light,
      CAST(vibration AS FLOAT) AS raw_vibration,
      CAST(noise     AS FLOAT) AS raw_noise,
      CAST(battery   AS FLOAT) AS raw_battery,
      CAST(dust      AS FLOAT) AS raw_dust,
      id,
      EventEnqueuedUtcTime AS event_time
```

```
    FROM [DataFromSensors]
    -- TIMESTAMP BY event_time
)
```

4.2 Згладження та попередня обробка даних

Після первинного зчитування даних із джерела необхідно виконати їх попередню обробку, щоб забезпечити точність подальшого аналізу та класифікації аномалій. Основним етапом цієї обробки є згладження даних за допомогою часових вікон, що дозволяє усунути шум і отримати більш стабільні значення для аналізу. Згладження реалізується через обчислення середніх, сум і підрахунків кількості записів у визначених часових інтервалах.

Для цього використовується оператор TUMBLINGWINDOW, який групує дані в інтервали часу тривалістю 30 секунд [25]. Обчислення середніх значень для кожного параметра дозволяє отримати більш наочну картину змін у часі, а підрахунок квадратів значень використовується для подальшого розрахунку Z-score. Крім того, враховується кількість записів у кожному інтервалі, що забезпечує достовірність обчислених статистик.

Приклад SQL-запиту для виконання цього етапу виглядає наступним чином:

```
WITH
Agg30s AS
(
    SELECT
        System.Timestamp() AS window_end_30s,
        id,
        AVG(raw_temp)          AS avg_temp_30s,
        AVG(raw_voltage)       AS avg_voltage_30s,
        AVG(raw_humidity)      AS avg_humidity_30s,
        AVG(raw_pressure)      AS avg_pressure_30s,
        AVG(raw_co2)           AS avg_co2_30s,
        AVG(raw_light)         AS avg_light_30s,
```

```
    AVG(raw_vibration)      AS avg_vibration_30s,
    AVG(raw_noise)          AS avg_noise_30s,
    AVG(raw_battery)        AS avg_battery_30s,
    AVG(raw_dust)           AS avg_dust_30s,
    -- Для Z-score рахуємо суму квадратів
    SUM(raw_temp*raw_temp)          AS sum_sq_temp,
    SUM(raw_voltage*raw_voltage)    AS sum_sq_volt,
    SUM(raw_humidity*raw_humidity)  AS sum_sq_humidity,
    SUM(raw_pressure*raw_pressure)  AS sum_sq_pressure,
    SUM(raw_co2*raw_co2)            AS sum_sq_co2,
    SUM(raw_light*raw_light)        AS sum_sq_light,
    SUM(raw_vibration*raw_vibration) AS sum_sq_vibration,
    SUM(raw_noise*raw_noise)        AS sum_sq_noise,
    SUM(raw_battery*raw_battery)    AS sum_sq_battery,
    SUM(raw_dust*raw_dust)          AS sum_sq_dust,
    COUNT(*) AS cnt_30s
  FROM InitialData
  GROUP BY TUMBLINGWINDOW(second, 30), id
)
```

На виході цього етапу ми отримуємо агреговані значення для кожного сенсора за 30-секундні інтервали. Ці дані служать основою для подальшої класифікації аномалій і виконання статистичних розрахунків. Використання такого підходу дозволяє враховувати динаміку змін параметрів, водночас мінімізуючи вплив короткочасних флуктуацій. Згладжені дані значно спрощують аналіз і підвищують точність виявлення аномальних подій.

4.3 Методи виявлення аномалій

Одним із ключових етапів класифікації є виявлення аномалій у даних, отриманих від сенсорів. Для цього в Stream Analytics Job застосовуються чотири основні методи: Spike&Dip, ChangePoint, ручна перевірка діапазонів (Manual Range

Check) і Z-score [26]. Кожен із цих методів має свою специфіку й підходить для різних сценаріїв виявлення відхилень у даних.

Метод Spike&Dip використовується для виявлення різких змін у значеннях параметрів, таких як раптові піки або провали. У Stream Analytics цей метод реалізується за допомогою функції AnomalyDetection_SpikeAndDip, яка враховує задані параметри чутливості (sensitivity) та порогу (threshold). Результатом роботи методу є об'єкт, що містить інформацію про те, чи була зафіксована аномалія [27]. Приклад використання методу:

```
AnomalyDetection_SpikeAndDip(avg_temp_30s, 80, 60, 'spikesanddips')
  OVER(PARTITION BY id LIMIT DURATION(second, 60)) AS spike_temp_obj
```

Метод ChangePoint спрямований на виявлення точок змін у трендах даних, наприклад, коли середні значення параметра різко зростають або знижуються. Це дозволяє ідентифікувати моменти, коли поведінка системи змінюється [28]. Реалізація методу виглядає наступним чином:

```
AnomalyDetection_ChangePoint(avg_temp_30s, 80, 60)
  OVER(PARTITION BY id LIMIT DURATION(second, 120)) AS change_temp_obj
```

Метод ручної перевірки дозволяє визначати аномалії, що виходять за межі заданого діапазону значень. Він реалізується через умовні конструкції CASE, які перевіряють, чи знаходиться значення в межах прийнятного інтервалу. Приклад перевірки:

```
CASE WHEN avg_temp_30s < 0 OR avg_temp_30s > 100 THEN 1 ELSE 0 END AS range_flag_temp
```

Метод Z-score базується на статистичному аналізі і дозволяє виявляти аномалії, які суттєво відхиляються від середнього значення [29]. Для розрахунку Z-

score спочатку обчислюється стандартне відхилення, а потім проводиться порівняння значення з середнім. Реалізація виглядає наступним чином:

```
CASE WHEN stdev_temp <> 0 AND ABS((avg_temp_30s - avg_temp_30s)/stdev_temp) > 3 THEN 1 ELSE 0 END AS zscore_flag_temp
```

Для кожного параметра сенсора застосовуються всі чотири методи виявлення аномалій, що дозволяє отримати комплексну картину. Результати виявлення зберігаються у вигляді окремих флагів для кожного методу. Це дає можливість аналізувати як окремі типи аномалій, так і їх комбінації, що підвищує точність і ефективність класифікації.

Застосування декількох методів одночасно забезпечує високу надійність і гнучкість системи, дозволяючи адаптувати її до різних сценаріїв і типів даних

4.4 Інтеграція результатів виявлення аномалій

Інтеграція результатів виявлення аномалій є критичним етапом, що забезпечує створення цілісної оцінки стану параметрів сенсорів на основі декількох методів аналізу. Результати кожного з методів – Spike&Dip, ChangePoint, Manual Range Check та Z-score – об'єднуються для формування остаточного висновку щодо наявності аномалій у даних. Цей підхід дозволяє враховувати різноманітні аспекти поведінки системи, забезпечуючи високу точність і надійність аналізу.

Для методів Spike&Dip і ChangePoint результати зберігаються у вигляді об'єктів, які містять властивість IsAnomaly. Ця властивість відображає, чи було виявлено аномалію для конкретного параметра. Для отримання цього значення використовується функція GetRecordPropertyValue. Наприклад, для параметра температури результат розпаковується наступним чином:

```
CAST(GetRecordPropertyValue(spike_temp_obj, 'IsAnomaly') AS BIGINT) AS spike_flag_temp,
```

```
    CAST(GetRecordPropertyValue(change_temp_obj, 'IsAnomaly') AS BIGINT) AS
change_flag_temp
```

Такі ж дії виконуються для кожного з параметрів сенсорів.

Окрім цього, результати ручної перевірки діапазонів та Z-score подаються у вигляді бінарних флагів, які показують, чи виходить значення за межі допустимих значень або суттєво відхиляється від середнього. Всі ці флаги інтегруються в єдину логіку для кожного параметра, що дозволяє формувати остаточний висновок. Наприклад, інтеграція результатів для температури виглядає так:

```
    CASE
      WHEN spike_flag_temp = 1 OR change_flag_temp = 1
          OR range_flag_temp = 1 OR zscore_flag_temp = 1 THEN 1
      ELSE 0
    END AS final_anomaly_flag_temp
```

Ця інтеграція гарантує, що навіть якщо аномалія була виявлена лише одним із методів, вона буде врахована в остаточному аналізі.

Після інтеграції результати групуються у часових вікнах для формування агрегованих показників. Це дозволяє оцінювати частоту аномалій за певний інтервал часу, що є важливим для моніторингу стабільності роботи системи. Наприклад, для 2-хвилинного вікна підрахунок кількості аномалій для кожного параметра виконується так:

```
    SELECT
      id,
      System.Timestamp() AS TimeBucket,
      COUNT(CASE WHEN final_anomaly_flag_temp = 1 THEN 1 END) AS
anomaly_count_temp,
      COUNT(CASE WHEN final_anomaly_flag_volt = 1 THEN 1 END) AS
anomaly_count_volt,
      ...
```

```
FROM FinalSelect
GROUP BY TUMBLINGWINDOW(minute, 2), id
```

На цьому етапі формується фінальний набір даних, який містить зведену інформацію про аномалії для кожного параметра у визначених часових інтервалах. Це дозволяє оперативно реагувати на аномалії та аналізувати їхні причини [30].

Таким чином, інтеграція результатів виявлення аномалій забезпечує створення цілісної картини стану системи. Використання декількох методів виявлення дозволяє враховувати різноманітні сценарії поведінки системи, що підвищує точність і надійність роботи алгоритму. Завдяки такому підходу можливо оперативно виявляти відхилення у роботі технологічних процесів та приймати обґрунтовані рішення щодо їх усунення.

4.5 Агрегування та аналіз результатів

Після інтеграції результатів виявлення аномалій виконується їхнє агрегування для створення зведених показників, що відображають загальну кількість та частоту спрацювань різних методів у визначених часових інтервалах. Цей етап є ключовим для забезпечення аналітичної обробки даних, оскільки дозволяє оцінювати стабільність роботи сенсорів і технологічного процесу в цілому.

Для агрегування даних застосовуються часові вікна, наприклад, тривалістю дві хвилини, у межах яких підраховується кількість аномалій для кожного параметра та методу [31]. Приклад реалізації такого підходу наведено нижче:

```
SELECT
   id,
   System.Timestamp() AS TimeBucket,
   -- Spike counts
   COUNT(CASE WHEN spike_flag_temp = 1 THEN 1 END) AS spike_temp_count,
   COUNT(CASE WHEN spike_flag_volt = 1 THEN 1 END) AS spike_volt_count,
```

```
    COUNT(CASE WHEN spike_flag_humidity = 1 THEN 1 END) AS spike_humidity_count,
    COUNT(CASE WHEN spike_flag_pressure = 1 THEN 1 END) AS spike_pressure_count,
    COUNT(CASE WHEN spike_flag_co2 = 1 THEN 1 END) AS spike_co2_count,
    ...
    -- ChangePoint counts
    COUNT(CASE WHEN change_flag_temp = 1 THEN 1 END) AS change_temp_count,
    COUNT(CASE WHEN change_flag_volt = 1 THEN 1 END) AS change_volt_count,
    COUNT(CASE WHEN change_flag_humidity = 1 THEN 1 END) AS
change_humidity_count,
    ...
    -- Range counts
    COUNT(CASE WHEN range_flag_temp = 1 THEN 1 END) AS range_temp_count,
    COUNT(CASE WHEN range_flag_volt = 1 THEN 1 END) AS range_volt_count,
    ...
    -- Z-score counts
    COUNT(CASE WHEN zscore_flag_temp = 1 THEN 1 END) AS zscore_temp_count,
    COUNT(CASE WHEN zscore_flag_volt = 1 THEN 1 END) AS zscore_volt_count,
    ...
FROM FinalSelect
GROUP BY TUMBLINGWINDOW(minute, 2), id
```

Цей запит дозволяє отримати кількість аномалій для кожного з параметрів у межах двохвилинного інтервалу. Такий підхід дозволяє виявити, які параметри мають підвищену частоту відхилень, а також зрозуміти, які методи найчастіше спрацьовують у даному часовому інтервалі.

Окрім кількісного підрахунку, на цьому етапі проводиться аналіз середніх значень для кожного параметра, щоб відстежувати їхню поведінку в часі. Наприклад:

```
AVG(avg_temp_30s) AS avg_temp_in_2m,
AVG(avg_voltage_30s) AS avg_voltage_in_2m,
```

Ці дані дозволяють побачити тренди параметрів у часовому інтервалі та зіставити їх із частотою виявлених аномалій. На основі цих результатів можна робити висновки про стабільність роботи обладнання та можливі причини відхилень.

Фінальним етапом є відбір часових інтервалів, у яких спрацював хоча б один із методів виявлення аномалій. Це дозволяє зосередити увагу на найбільш критичних періодах, що потребують детального аналізу. Приклад відбору:

```
SELECT *
FROM AggregatedResults
WHERE spike_temp_count > 0 OR change_temp_count > 0 OR range_temp_count > 0 OR zscore_temp_count > 0
ORDER BY TimeBucket DESC
```

Цей запит відбирає лише ті інтервали часу, у яких були зафіксовані аномалії, що спрощує подальший аналіз і дозволяє ефективно виявляти проблемні зони.

Таким чином, агрегування та аналіз результатів дозволяють створити зведену картину стану системи, оцінити частоту й характер аномалій, а також підготувати дані для подальшого глибшого аналізу чи автоматизованого реагування на відхилення.

4.6 Висновки до четвертого розділу

У цьому розділі було розглянуто весь процес обробки даних у Stream Analytics Job для класифікації аномалій. Було детально описано етапи обробки – від первинного зчитування та згладження даних до інтеграції результатів виявлення аномалій і їхнього агрегування. Кожен із методів виявлення аномалій, таких як Spike&Dip, ChangePoint, ручна перевірка діапазонів і Z-score, має свою специфіку, що дозволяє виявляти різноманітні відхилення в даних.

Особливу увагу було приділено інтеграції результатів усіх методів для створення цілісної картини стану кожного параметра. Завдяки цьому вдалося

забезпечити комплексний підхід до аналізу аномалій, що дозволяє ефективно виявляти відхилення навіть у випадках, коли вони неочевидні при використанні окремих методів.

Агрегування результатів виявлення аномалій у часових вікнах забезпечує зручний формат для подальшого аналізу, дозволяючи відстежувати частоту й характер аномалій у часі. Це створює основу для глибшого аналізу, автоматизованого реагування на відхилення та прийняття рішень, спрямованих на усунення причин аномалій.

Таким чином, розглянутий підхід демонструє ефективність використання SQL-запитів у Stream Analytics Job для обробки потокових даних і класифікації аномалій, забезпечуючи точність, гнучкість і масштабованість системи [32-33].

5 ЕКСПЕРИМЕНТАЛЬНИЙ АНАЛІЗ РОБОТИ СИСТЕМИ ВИЯВЛЕННЯ АНОМАЛІЙ

5.1 Аналіз роботи штучних датчиків

Система виявлення аномалій включає етап генерації даних, який здійснюється за допомогою штучних датчиків. Ці сенсори дозволяють створювати потокові дані, що відповідають реальним показникам роботи обладнання, включаючи температуру, напругу, вологість, тиск, рівень CO2, освітленість, вібрацію, шум, заряд батареї та рівень пилу. Генерація даних реалізується через спеціалізований симулятор, який забезпечує можливість створення як нормальних, так і аномальних значень для тестування алгоритмів виявлення аномалій [34]. Інтерфейс симулятора представлений на рис. 5.1.

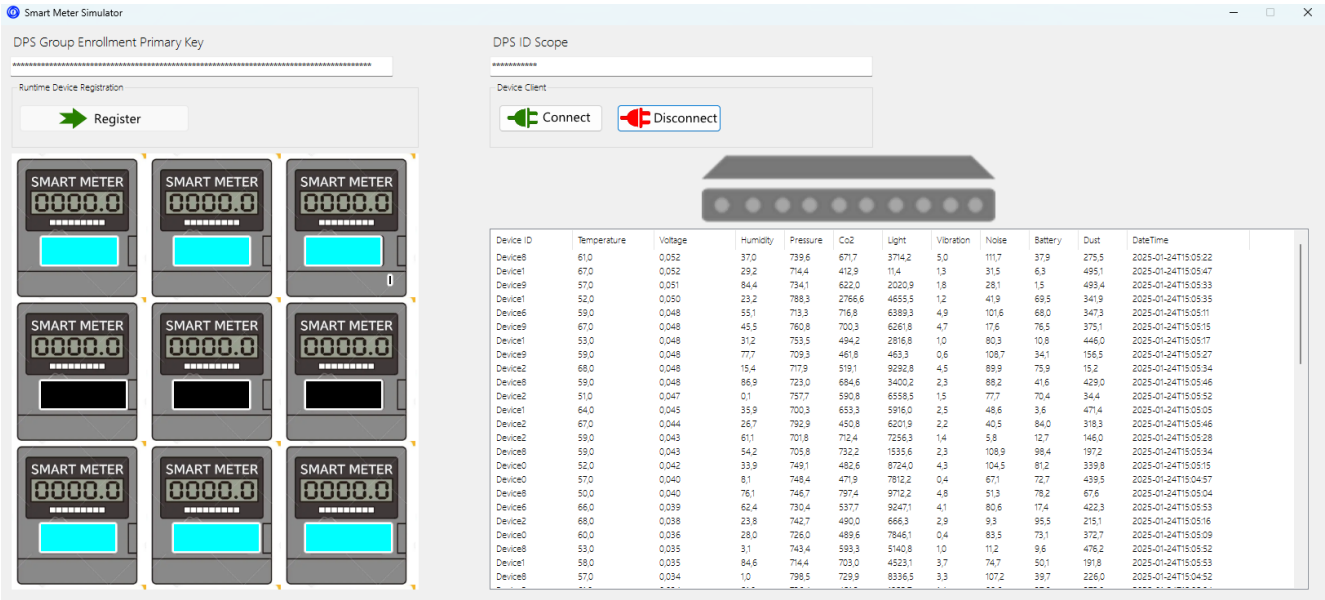

Рисунок 5.1 – Інтерфейс симулятора

Ліва частина інтерфейсу відображає дев'ять віртуальних пристроїв, які імітують роботу розумних лічильників (Smart Meter). Кожен лічильник може окремо вмикатися, вимикатися та відповідно генерувати дані.

У верхній частині вікна передбачено поле для введення первинного ключа групового реєстрування DPS (Device Provisioning Service), яке забезпечує можливість підключення пристроїв до хмарного сервісу Azure. Для реєстрації пристроїв реалізована кнопка «Register», яка дозволяє додавати сенсори до групи, а також ініціювати процес генерації даних. Варто зауважити, щоб зареєструвати пристрій потрібно спочатку натиснути на велику чорнку кнопку на самому пристрої, щоб привести його у активний режим і лише після цього реєструвати.

Права частина інтерфейсу демонструє табличний вигляд зібраних даних. Тут відображаються всі ключові параметри для кожного сенсора, включаючи ідентифікатор пристрою (Device ID), значення параметрів (наприклад, температура, напруга тощо) та часову мітку (DateTime). Ця таблиця забезпечує можливість моніторингу змін показників у реальному часі.

Секція «DPS ID Scope» у верхній правій частині інтерфейсу дозволяє встановлювати з'єднання між симулятором і Azure IoT Hub за допомогою кнопок «Connect» та «Disconnect». Це забезпечує передачу даних від симулятора до хмарної платформи для подальшої обробки та аналізу.

Застосування симулятора дозволяє створити повноцінну модель роботи сенсорів у контрольованому середовищі, що сприяє детальному аналізу їх поведінки. Це також забезпечує можливість оцінити якість згенерованих даних, перевірити алгоритми обробки та протестувати взаємодію сенсорів із зовнішніми системами, такими як хмарні платформи. Такий підхід сприяє підвищенню надійності та точності системи, дозволяючи виявити потенційні проблеми ще на етапі розробки.

5.2 Аналіз інтеграції та роботи в Azure

У цьому підрозділі розглянуто інтеграцію симулятора з хмарними сервісами Azure, включаючи роботу з IoT Hub, Stream Analytics та іншими компонентами, які забезпечують збір, обробку й аналіз даних.

На рис. 5.2 представлено загальний огляд проєкту в Azure. Тут відображені ресурси, створені для підтримки системи, такі як IoT Hub, Device Provisioning Service, Stream Analytics Job, Storage Account та інші компоненти. Даний вигляд дозволяє контролювати всі ресурси в рамках одного підрозділу, включаючи загальну вартість підписки [35-36]. Також він відображає приблизну вартість витрачених коштів на платні сервіси. Приблизну, оскільки певні підпискові моделі виставляють свої рахунки в кінці місяця, відповідно тоді і додаються до суми.

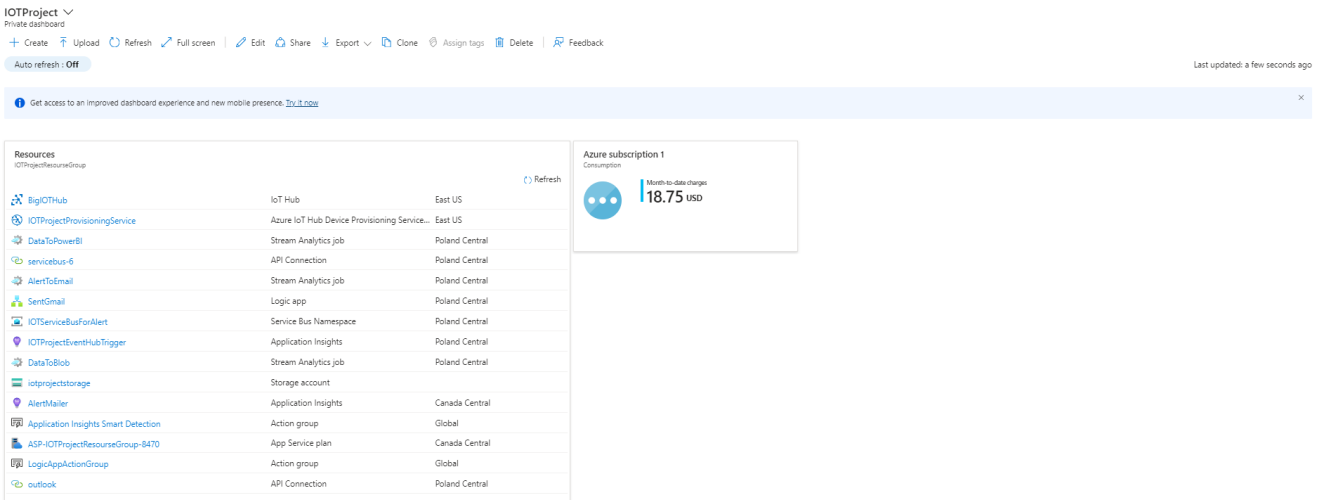

Рисунок 5.2 – Azure dashboard

На рис. 5.3 показано роботу служби Device Provisioning Service (DPS). Вона використовується для реєстрації сенсорів у системі. На зображенні видно прив’язку до IoT Hub, що забезпечує подальшу обробку даних, зібраних пристроями.

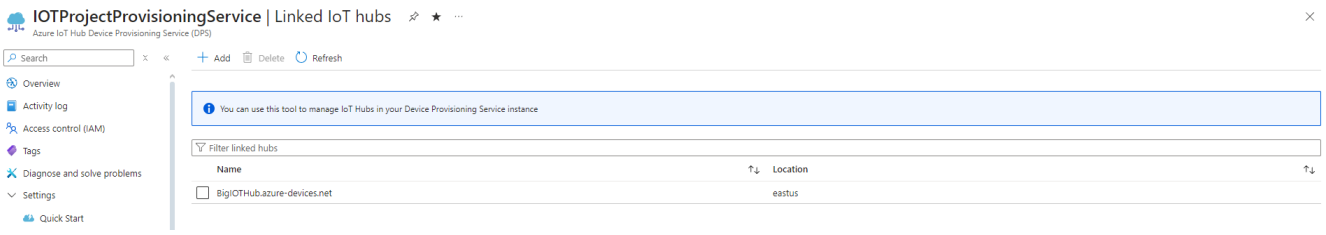

Рисунок 5.3 – Azure IoT Hub DPS

Рис. 5.4 демонструє список пристроїв, підключених до IoT Hub. Для кожного пристрою відображається його статус, тип аутентифікації (Shared Access Signature) та кількість повідомлень, що очікують на обробку. Це дозволяє здійснювати моніторинг підключених пристроїв і стан їх роботи.

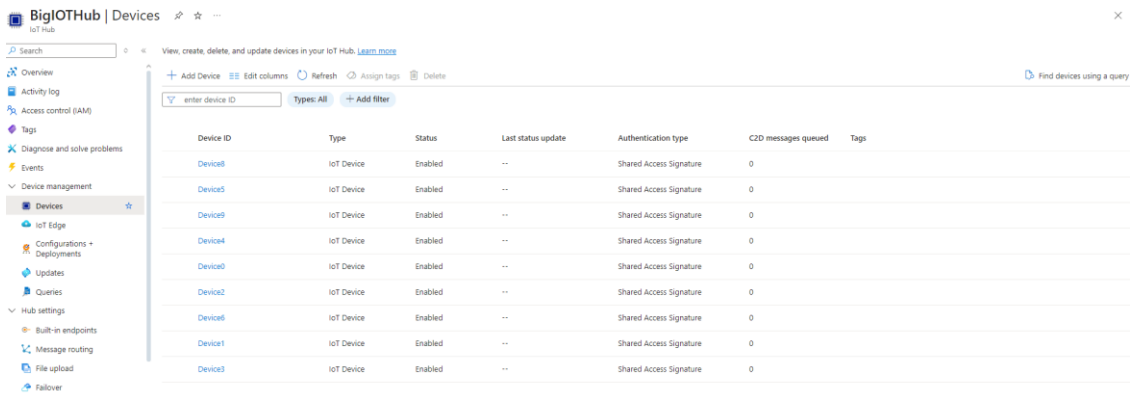

Рисунок 5.4 – Azure IoT Hub

На рис. 5.5 представлені ключові метрики роботи IoT Hub. Тут видно кількість підключених пристроїв, використання повідомлень на день і обсяг телеметричних даних, що передаються до хмари. Дана інформація є важливою для оцінки продуктивності системи.

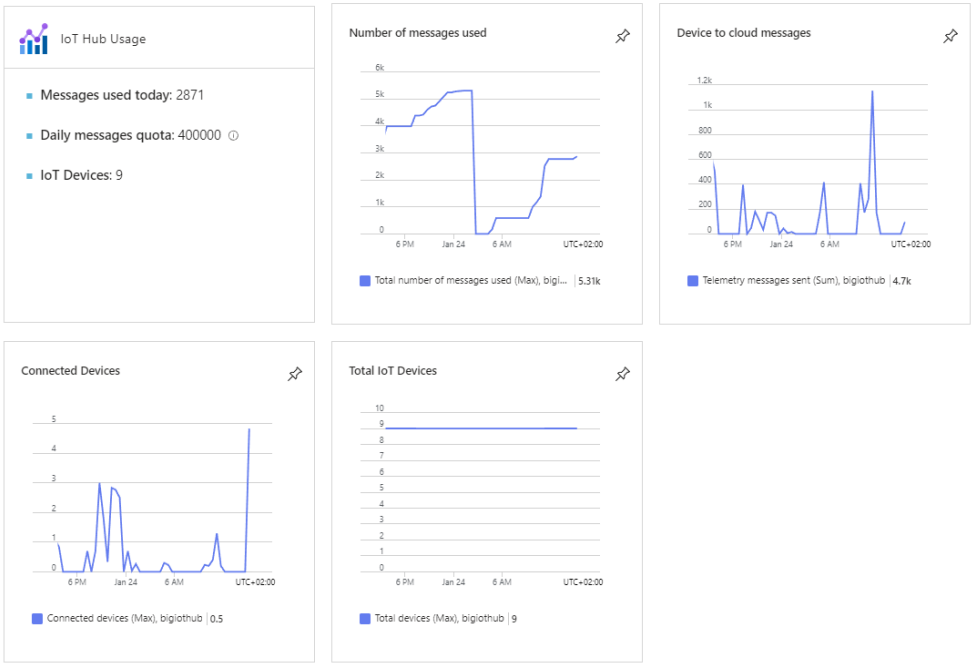

Рисунок 5.5 – Показники роботи Azure IoT Hub

На рис. 5.6, зображені метрики Stream Analytics Job. Графіки відображають використання ресурсів, кількість вхідних і вихідних подій, затримки обробки та можливі помилки. Аналіз цих даних дозволяє оцінити продуктивність потоку аналітики та визначити точки оптимізації.

Рисунок 5.6 – Показники роботи Stream Analytics Job

На рис. 5.7 наведено приклад файлу збережених даних у Storage Account. Цей файл містить телеметрію від сенсорів, включаючи часові мітки та показники, які передаються до IoT Hub. Файл зберігається у форматі CSV для зручності подальшого аналізу.

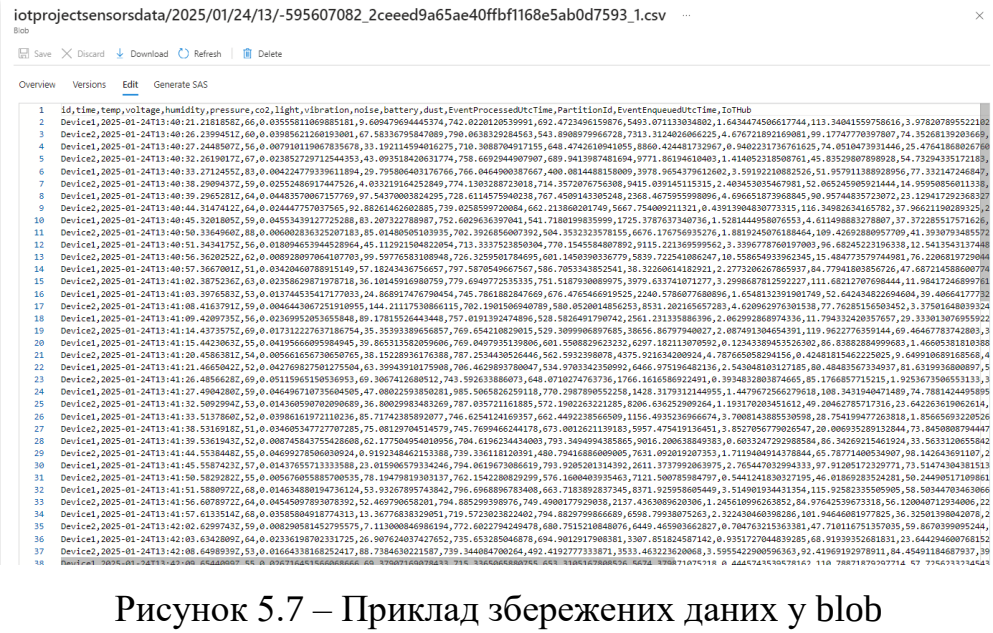

Рисунок 5.7 – Приклад збережених даних у blob

Рис. 5.8 відображає роботу Service Bus, який використовується для передачі повідомлень про аномалії. Графіки відображають обробку вхідних і вихідних повідомлень, що дозволяє контролювати потоки даних у реальному часі.

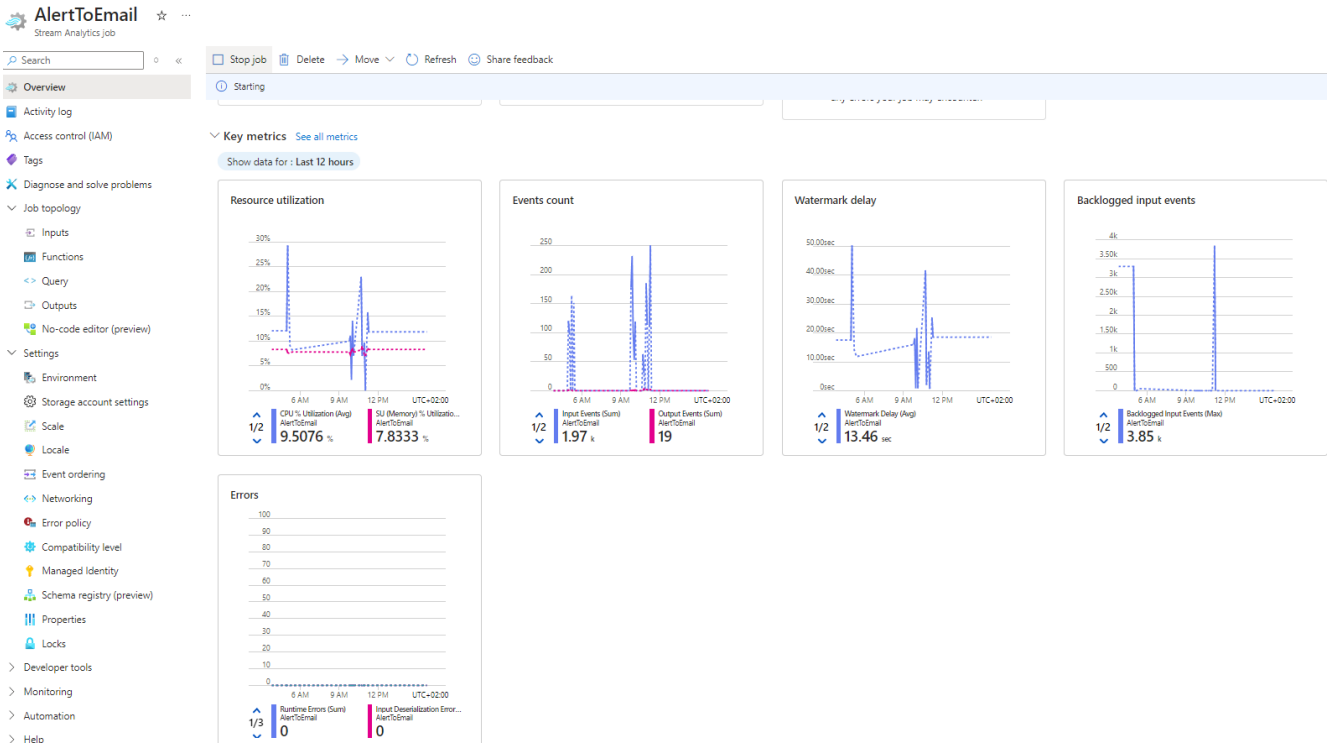

Рисунок 5.8 – Показники роботи Stream Analytics Job

На рис. 5.9 зображено зміст повідомлення, яке надходить до Service Bus. У повідомленні містяться агреговані результати аналізу аномалій, що дозволяє швидко оцінити стан системи.

Рисунок 5.9 – Message body у Bus Queue

На рис. 5.10 зображено отримане сповіщення на електронну пошту про виявлення аномалії в роботі пристрою. Це підтверджує успішну інтеграцію системи з механізмами оповіщення.

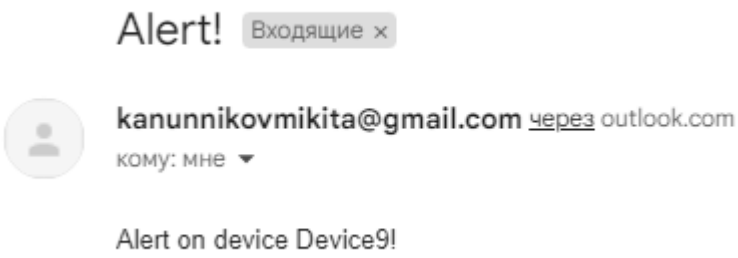

Рисунок 5.10 – Приклад email повідомлення з вказанням на якому пристрої аномалія

На рис. 5.11 наведено метрики роботи іншого Stream Analytics Job, який відповідає за передачу даних у PowerBI. Як видно, метрики містять інформацію про використання ресурсів, кількість оброблених подій, затримки обробки (Watermark Delay) та кількість подій, які очікують на обробку (Backlogged Input Events). Це дозволяє оцінити ефективність потоку аналітики та стабільність обробки даних, які надсилаються для візуалізації.

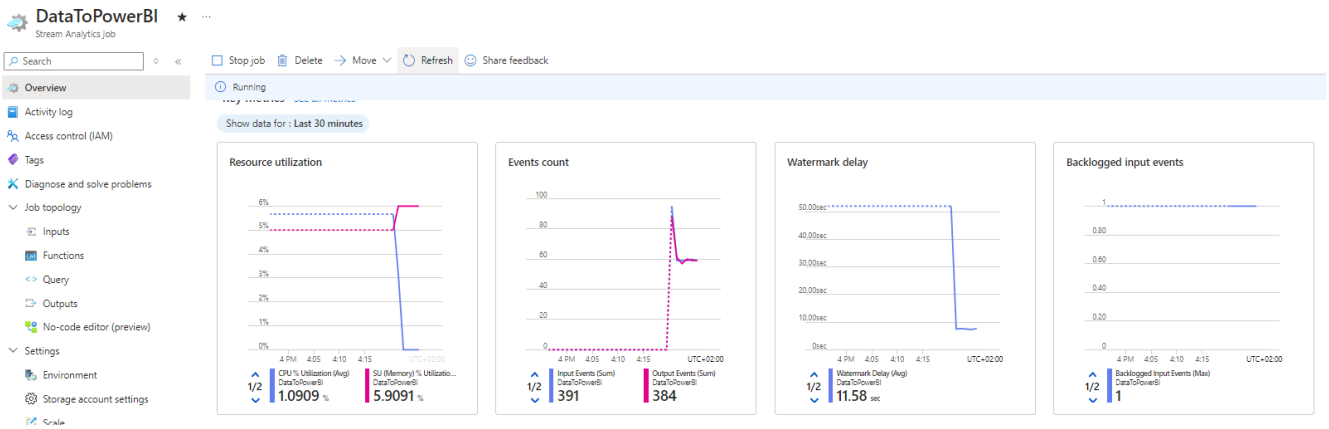

Рисунок 5.11 – Показники роботи Stream Analytics Job

На рис. 5.12 зображено приклади графіків у Power BI, створених на основі переданих даних. Графіки відображають середні значення ключових параметрів, таких як заряд батареї, рівень CO2, шум, пил, освітленість, тиск, температура та вібрація для кожного пристрою. Ця візуалізація дає змогу швидко оцінити стан кожного з пристроїв та порівняти їх між собою.

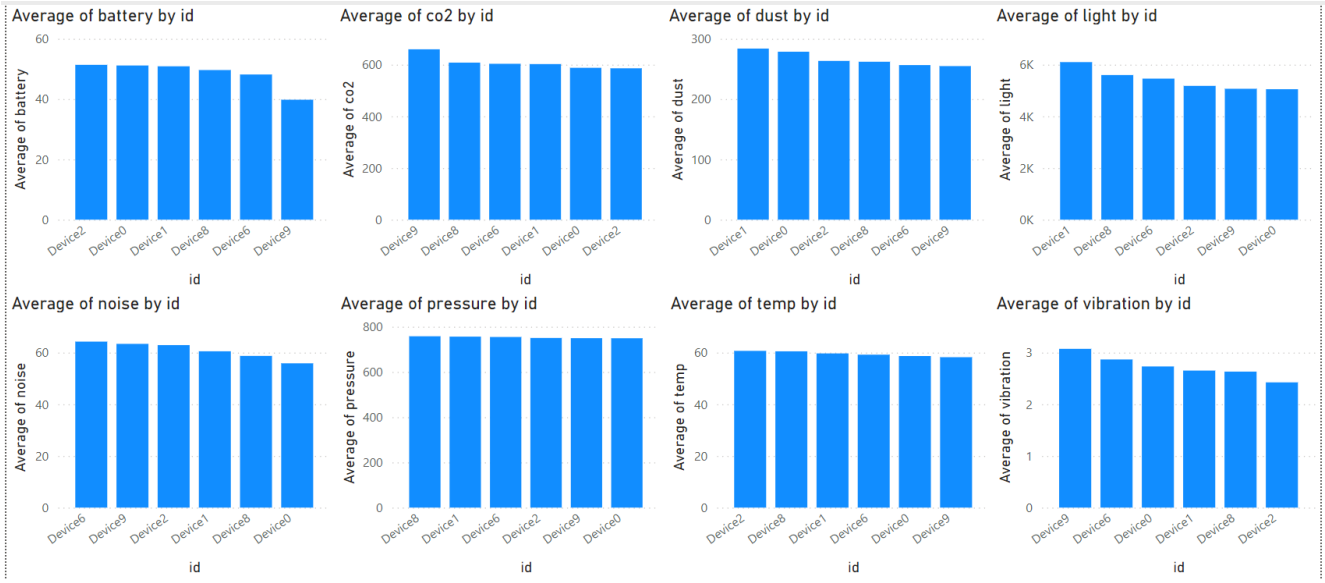

Рисунок 5.12 – Агрегаційні графіки середніх значень показників по пристроям

5.3 Висновки до п’ятого розділу

У п’ятому розділі було проведено експериментальний аналіз роботи системи виявлення аномалій, який охоплював два основні аспекти: роботу штучних сенсорів і інтеграцію з хмарними сервісами Azure. Було продемонстровано ефективність симулятора для генерації даних, зокрема його здатність створювати телеметричні дані з аномальними значеннями, що дозволило протестувати роботу алгоритмів виявлення аномалій у контрольованих умовах [37-40].

Інтеграція з Azure, зокрема використання IoT Hub, Device Provisioning Service та Stream Analytics, забезпечила стабільну обробку та передачу даних у реальному часі. Результати обробки були візуалізовані у Power BI, що підтвердило можливість використання системи для моніторингу параметрів сенсорів і оцінки їхнього стану. Було також продемонстровано роботу Service Bus для оповіщення про виявлені

аномалії через електронну пошту, що підтверджує здатність системи оперативно реагувати на критичні ситуації.

Експериментальні результати показали, що система є масштабованою, продуктивною та надійною для вирішення задач моніторингу й аналізу технологічних процесів у реальному часі. Це створює основу для подальшого вдосконалення алгоритмів обробки та інтеграції системи в промислові середовища.

6 БЕЗПЕКА КОРИСТУВАЧІВ У СИСТЕМАХ МОНІТОРИНГУ

6.1 Ризики для користувачів у системах моніторингу

Системи моніторингу технологічних процесів, хоча й забезпечують значні переваги, мають потенційні ризики для користувачів. Одним із ключових ризиків є витік конфіденційних даних. У системах, що працюють із сенсорними даними, інформація про стан технологічного процесу або пристроїв може містити критично важливі для організації відомості. У разі компрометації такої інформації зловмисники можуть використати її для шкідливих цілей, наприклад, промислового шпигунства або створення загроз безпеці [41].

Другим важливим ризиком є несанкціонований доступ до системи. Якщо зловмисники отримають доступ до інтерфейсу управління системою або до її ключових компонентів, вони можуть маніпулювати даними, виводити з ладу пристрої або навіть змінювати параметри їхньої роботи, створюючи небезпечні умови для користувачів.

Ще одним ризиком є помилкова тривога. У системах моніторингу аномалій помилкові сигнали можуть викликати стрес у користувачів, призводити до надмірної витрати ресурсів на перевірку й усунення неіснуючих проблем або навіть викликати зниження довіри до системи.

Також варто враховувати ризики, пов’язані із фізичною безпекою користувачів. У разі некоректної роботи системи чи її компонентів можуть виникати загрози здоров’ю або життю працівників, які взаємодіють із технологічними процесами.

Загалом, розуміння та врахування цих ризиків є необхідним для забезпечення безпеки користувачів. Це дозволяє системі працювати ефективно й надійно, мінімізуючи потенційні загрози.

6.2 Методи аутентифікації та захисту користувачів

Аутентифікація є ключовим компонентом безпеки в системах моніторингу, особливо в тих, що інтегровані з хмарними платформами, такими як Azure. У даній системі використано сучасні методи автентифікації, зокрема логіни та паролі, які застосовуються для захисту доступу до критично важливих ресурсів, таких як IoT Hub та Device Provisioning Service.

Azure підтримує багаторівневу аутентифікацію, що включає обов’язкове використання паролів із високим рівнем складності. Паролі створюються з урахуванням сучасних стандартів безпеки, включаючи мінімальну довжину, обов’язкове використання великих і малих літер, цифр і спеціальних символів. Це зменшує ризик підбору паролів або несанкціонованого доступу.

Крім того, для автентифікації пристроїв у системі застосовується метод Shared Access Signature (SAS) [42]. SAS дозволяє створювати тимчасові токени доступу, які забезпечують передачу даних від сенсорів до IoT Hub. Це мінімізує ризики компрометації ключів, оскільки вони регулярно оновлюються і мають обмежений термін дії.

Для додаткового захисту користувачів у хмарній інфраструктурі використовується багатофакторна аутентифікація (MFA). MFA вимагає, окрім введення пароля, підтвердження особи за допомогою другого фактора, наприклад, коду, відправленого на мобільний пристрій, або біометричних даних. Це значно знижує ймовірність несанкціонованого доступу навіть у випадку компрометації пароля.

Для управління правами доступу в системі застосовується рольова модель (Role-Based Access Control, RBAC). Вона дозволяє надавати користувачам лише ті права, які необхідні для виконання їхніх завдань, наприклад, доступ до аналітичних даних або моніторинг пристроїв, без можливості змінювати критичні налаштування.

Таким чином, використання комплексного підходу до автентифікації та захисту користувачів у системі моніторингу, що включає логіни, паролі, SAS-

токени, MFA та RBAC, забезпечує високий рівень безпеки і мінімізує ризики несанкціонованого доступу до даних і ресурсів.

6.3 Забезпечення конфіденційності даних користувачів

Конфіденційність даних є одним із найважливіших аспектів у системах моніторингу, особливо коли йдеться про зберігання і передачу інформації про технологічні процеси та користувачів. У даній системі використовуються сучасні підходи, спрямовані на захист інформації від несанкціонованого доступу, витоку чи зміни.

Для забезпечення конфіденційності під час передачі даних використовується протокол шифрування TLS (Transport Layer Security) [43]. TLS гарантує захищений канал між пристроями й хмарною інфраструктурою, зокрема між сенсорами та IoT Hub. Це забезпечує цілісність і захист даних навіть у разі їхнього перехоплення.

Усі дані, які зберігаються в Azure Blob Storage, шифруються на рівні зберігання (encryption-at-rest). Ця функціональність дозволяє автоматично шифрувати файли під час їхнього запису та розшифровувати під час зчитування. Таким чином, дані залишаються захищеними навіть у разі компрометації доступу до сховища.

Для обмеження доступу до конфіденційної інформації застосовується модель Role-Based Access Control (RBAC). Вона дозволяє чітко розмежувати рівні доступу для різних груп користувачів. Наприклад, адміністратори можуть мати доступ до налаштувань системи, тоді як аналітики отримують лише доступ до результатів обробки даних.

Окрім цього, система забезпечує аудит усіх дій із даними через логування активності. Це дозволяє виявити й попередити спроби несанкціонованого доступу або зміни критично важливої інформації. Логи активності регулярно перевіряються, а в разі виявлення аномалій система може автоматично повідомити адміністратора.

Додатковий рівень конфіденційності забезпечується через мінімізацію зберігання персональних даних користувачів. Уся інформація, яка не є критично необхідною для роботи системи, видаляється або анонімізується, знижуючи ризики витоку конфіденційних даних.

Забезпечення конфіденційності даних у даній системі сприяє побудові довіри серед користувачів і підвищенню загального рівня безпеки. Використання сучасних технологій і практик дозволяє захистити дані як у процесі їхньої обробки, так і під час зберігання.

6.4 Навчання користувачів безпечної роботи з системою

Ефективна система безпеки неможлива без навчання користувачів. Забезпечення їх обізнаності у сфері кібербезпеки допомагає зменшити кількість помилок, які можуть призвести до загроз для даних і технологічних процесів. У даній системі особливу увагу приділено проведенню інструктажів і тренінгів для користувачів, що взаємодіють із системою моніторингу.

Одним із ключових аспектів навчання є ознайомлення з основними принципами створення та зберігання надійних паролів. Користувачі повинні розуміти важливість використання складних паролів і необхідність їх регулярної зміни. Крім того, проводяться інструкції щодо правильного використання двофакторної аутентифікації (MFA) для захисту облікових записів.

Іншим важливим компонентом є навчання користувачів розпізнаванню потенційних загроз, таких як фішингові атаки або підозрілі повідомлення.

Додатково, користувачі повинні проходити інструктаж із роботи з інтерфейсом системи моніторингу. Їм пояснять, як правильно інтерпретувати дані, отримані від сенсорів, і як діяти у разі отримання сповіщень про аномалії. Це дозволяє мінімізувати кількість помилкових рішень, що можуть вплинути на безпеку процесів.

Система також передбачає надання регулярних оновлень щодо змін у безпековій політиці та нових загроз. Користувачі повинні отримувати доступ до

онлайн-ресурсів із рекомендаціями щодо безпечної роботи, а також до відеоматеріалів і вебінарів, присвячених актуальним темам кібербезпеки.

Навчання користувачів безпечної роботи з системою є невід'ємною частиною забезпечення безпеки [44]. Завдяки регулярним тренінгам і доступу до освітніх ресурсів, користувачі стають активними учасниками захисту системи, що значно підвищує її надійність і захищеність.

6.5 Висновки до шостого розділу

Розділ розкрив основні аспекти забезпечення безпеки користувачів у системах моніторингу. Було розглянуто ризики, пов'язані з використанням таких систем, включаючи витік даних, несанкціонований доступ, помилкові тривоги та неправильну інтерпретацію даних. Особливу увагу приділено методам автентифікації та захисту користувачів, серед яких використання складних паролів, двофакторної аутентифікації, SAS-токенів і рольової моделі доступу [45].

Також було підкреслено важливість забезпечення конфіденційності даних за допомогою протоколів TLS, шифрування даних у сховищах та обмеження доступу на основі ролей. Додатково, система забезпечує логування активності користувачів, що дозволяє моніторити й запобігати спробам несанкціонованого доступу.

Особливої уваги заслуговує навчання користувачів безпечній роботі з системою. Проведення регулярних інструктажів і тренінгів сприяє підвищенню обізнаності користувачів щодо кібербезпеки, мінімізує ризики людських помилок та зміцнює загальний рівень захисту.

Загалом, запропоновані заходи дозволяють створити надійну й захищену систему моніторингу, що забезпечує безпеку як користувачів, так і даних. Використання сучасних технологій і підходів до безпеки сприяє підвищенню довіри до системи та її ефективності в реальних умовах.

ВИСНОВКИ

У процесі виконання кваліфікаційної роботи було розроблено систему моніторингу та прогнозування стану технологічних процесів, що поєднує в собі сучасні методи обробки даних, механізми виявлення аномалій і інтеграцію з хмарними сервісами. Основним завданням роботи було створення ефективної, масштабованої та безпечної системи, яка б забезпечувала виявлення потенційних проблем у роботі технологічного обладнання, запобігаючи можливим відмовам і збоям.

На першому етапі було розроблено симулятор сенсорних даних, який дозволяє генерувати телеметричні показники в реальному часі. Унікальність цього симулятора полягає у здатності імітувати як нормальні умови роботи пристроїв, так і різні типи аномалій. Це забезпечило можливість перевірки роботи алгоритмів виявлення відхилень у контрольованому середовищі. До основних параметрів, які симулювалися, входили температура, напруга, вологість, тиск, рівень CO2, освітленість, вібрація, шум, заряд батареї та рівень пилу. Алгоритми створення аномалій дозволили моделювати реальні умови роботи технологічного обладнання, забезпечуючи високу точність тестування системи.

Інтеграція симулятора з хмарною платформою Azure дала змогу забезпечити стабільну передачу, обробку й зберігання телеметричних даних. Використання таких сервісів, як Azure IoT Hub, Device Provisioning Service, Stream Analytics та Azure Blob Storage, дозволило створити ефективну інфраструктуру для роботи з великими потоками даних у реальному часі. Зокрема, Stream Analytics Job продемонстрував свою ефективність у виявленні аномалій за допомогою методів Spike&Dip, ChangePoint, Manual Range Check та Z-score. Отримані результати аналізу були успішно інтегровані з Power BI для створення зручних і наочних візуалізацій, що сприяє прийняттю оперативних рішень.

Особлива увага в роботі була приділена забезпеченню безпеки системи. Для цього було впроваджено багаторівневі механізми автентифікації користувачів,

включаючи складні паролі, SAS-токени та двофакторну аутентифікацію. Крім того, застосування шифрування TLS під час передачі даних і encryption-at-rest для їх зберігання гарантує конфіденційність і захист інформації від витоків. Важливою складовою також стало навчання користувачів безпечній роботі з системою, що сприяє зниженню ризиків, пов'язаних із людським фактором.

Експериментальний аналіз роботи системи підтвердив її ефективність і надійність. Було продемонстровано, що система здатна виявляти потенційні аномалії в режимі реального часу, забезпечуючи високу точність і швидкість обробки даних. Візуалізація результатів у Power BI дозволяє користувачам швидко оцінювати стан обладнання та приймати обґрунтовані рішення. Важливо відзначити, що система показала свою масштабованість і адаптивність, що дозволяє інтегрувати її в різні технологічні середовища.

Під час реалізації системи були враховані сучасні підходи до обробки даних, які можуть бути розширені відповідно до вимог конкретного виробничого середовища. Зокрема, додавання нових алгоритмів аналізу або інтеграція з іншими сервісами Azure дозволить удосконалювати систему для більш складних сценаріїв використання.

Підсумовуючи, виконана робота демонструє можливість створення сучасної системи моніторингу та прогнозування стану технологічних процесів, яка поєднує в собі гнучкість, масштабованість, безпеку та зручність у використанні. Розроблена система може бути адаптована до різних типів обладнання та сфер застосування, що робить її універсальним інструментом для підтримки стабільності та безпеки технологічних процесів. Використання хмарних технологій та інтеграція з передовими методами обробки даних створює перспективи для подальшого розвитку і вдосконалення системи, орієнтованої на потреби сучасного виробництва.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Методичні вказівки з підготовки та захисту кваліфікаційної роботи здобувачами другого (магістерського) рівня вищої освіти спеціальності 174 Автоматизація, комп'ютерно-інтегровані технології та робототехніка, освітньо-професійних програм: «Комп'ютерно-інтегровані технологічні процеси і виробництва», «Комп'ютеризовані та робототехнічні системи» / Упоряд. І. Ш. Невлюдов, Р. В. Артюх, В. В. Безкоровайний, Н. П. Демська, В. В. Євсєєв, О. І. Филипенко, О. М. Цимбал. Харків: ХНУРЕ, 2024. 57 с.

2. ДСТУ 3008-15. Інформація та документація. Звіти у сфері науки та техніки. Структура та правила оформлювання. / Нац. стандарт України. – Вид. офіц. – [Чинний від 2015-06-22]. – Київ: Держстандарт України, 2017. – 26 с.

3. Положення про академічну доброчесність [Електронний ресурс]: наказ ХНУРЕ від 02 лютого 2021 р. № 50. – Режим доступу: https://nure.ua/wpcontent/uploads/Main_Docs_NURE/polozhennja-pro-akademi-chnu-dobrochesnist.pdf.

4. Основи наукових досліджень : підручник / І. Ш. Невлюдов, Ю. М. Олександров, А. О. Андрусевич, О. О. Чала ; М-во освіти і науки України, Харків. нац. ун-т радіоелектроніки. – Prague : OKTAN PRINT, 2024. – 468 с.

5. Ullo S. L., Sinha G. R. Advances in smart environment monitoring systems using IoT and sensors / S. L. Ullo, G. R. Sinha // Sensors. – 2020. – Vol. 20, № 11. – Article 3113.

6. Yadav G., Paul K. Architecture and security of SCADA systems: A review / G. Yadav, K. Paul // International Journal of Critical Infrastructure Protection. – 2021. – Vol. 34. – Article 100433.

7. Nevliudov, I., & et al.. (2020). Method of Algorithms for Cyber-Physical Production Systems Functioning Synthesis. International Journal of Emerging Trends in Engineering Research, 8(10), 7465-7473.

8. Laha S. R., Pattanayak B. K., Pattnaik S. Advancement of environmental monitoring system using IoT and sensor: A comprehensive analysis / S. R. Laha, B. K. Pattanayak, S. Pattnaik // AIMS Environmental Science. – 2022. – Vol. 9, № 6. – P. 771–800.

9. Невлюдов І.Ш. Виробничі процеси та обладнання об’єктів автоматизації. Збірник задач: Навчальний посібник / І.Ш. Невлюдов, А.О. Андрусевич, Г.В. Пономарьова, А.О. Функендорф. Кривий Ріг: КК НАУ. 2018. – 332 с.

10. Napoleone A., Macchi M., Pozzetti A. A review on the characteristics of cyber-physical systems for the future smart factories / A. Napoleone, M. Macchi, A. Pozzetti // Journal of Manufacturing Systems. – 2020. – Vol. 54. – P. 305–335.

11. Andersson J. C. Learning Microsoft Azure / J. C. Andersson. – Sebastopol: O'Reilly Media, Inc., 2023.

12. Palumbo F., et al. Characterization and analysis of cloud-to-user latency: The case of Azure and AWS / F. Palumbo, et al. // Computer Networks. – 2021. – Vol. 184. – Article 107693.

13. Borra P. Advancing Data Science and AI with Azure Machine Learning: A Comprehensive Review / P. Borra // International Journal of Research Publication and Reviews. – 2024. – Vol. 5, № 6. – P. 1825–1831.

14. Soh J., et al. Microsoft Azure: Planning, Deploying, and Managing the Cloud / J. Soh, et al. – New York, NY, USA : Apress, 2020.

15. Теорія автоматичного управління (збірник задач) [Текст]: навч.посіб. для студентів спеціальності 151 Автоматизація та комп'ютерно-інтегровані технології / І.Ш. Невлюдов, О.В. Токарєва; Харків. нац. ун-т радіоелектроніки. - Харків: Панов А.М., 2020. – 240 с.

16. Штіфзон О. Й., Новіков П. В., Бунь В. П. Теорія автоматичного управління : навч. посіб. / О. Й. Штіфзон, П. В. Новіков, В. П. Бунь. – 2020.

17. Мураховський С. А., Півторак Д. О. Теорія автоматичного управління. Теорія лінійних систем автоматичного управління / С. А. Мураховський, Д. О. Півторак. – 2022.

18. Невлюдов І.Ш. Комп’ютерно-інтегровані технології виробництва технічних засобів автоматизації. Частина 1: підручник. Харків: ФОП Панов А.М., 2021. – 604 с.

19. Mishra B., Kertesz A. The use of MQTT in M2M and IoT systems: A survey / B. Mishra, A. Kertesz // IEEE Access. – 2020. – Vol. 8. – P. 201071–201086.

20. Bender M., et al. Open-source MQTT evaluation / M. Bender, et al. // 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC). – IEEE, 2021.

21. Pliatsios D., et al. A survey on SCADA systems: secure protocols, incidents, threats and tactics / D. Pliatsios, et al. // IEEE Communications Surveys & Tutorials. – 2020. – Vol. 22, № 3. – P. 1942–1976.

22. Maksymova S. The Monitoring System Architecture Development / S. Maksymova, V. Yevsieiev, Ahmad Alkhalaileh // Journal of Universal Science Research, 2024. – Vol. 2(1). – P. 69–79.

23. Nagasubramanian G., et al. Ensemble classification and IoT-based pattern recognition for crop disease monitoring system / G. Nagasubramanian, et al. // IEEE Internet of Things Journal. – 2021. – Vol. 8, № 16. – P. 12847–12854.

24. Mauri D., Coriani S., Hoffman A., Mishra S., Popovic J. Practical Azure SQL Database for Modern Developers / D. Mauri, S. Coriani, A. Hoffman, S. Mishra, J. Popovic. – Berkeley, CA, USA : Apress, 2021.

25. Mauri D., Coriani S., Hoffman A., Mishra S., Popovic J. Azure SQL Kickstart. Practical Azure SQL Database for Modern Developers: Building Applications in the Microsoft Cloud / D. Mauri, S. Coriani, A. Hoffman, S. Mishra, J. Popovic. – 2021. – P. 15–34.

26. L’Esteve R. C. Stream Analytics Anomaly Detection / R. C. L’Esteve // The Definitive Guide to Azure Data Engineering: Modern ELT, DevOps, and Analytics on the Azure Cloud Platform. – Berkeley, CA : Apress, 2021. – P. 349–381.

27. Georgiev G., Portela R., Bañares M. A., Coca-Lopez N. Spike detection algorithms for Raman spectroscopy: a comparative study / G. Georgiev, R. Portela, M.

A. Bañares, N. Coca-Lopez // Data Science for Photonics and Biophotonics : Proc. of SPIE Conf., 18 Jun. 2024. – Vol. 13011. – P. 24–28.

28. Volkovičs R. Anomaly Detection: Review of Methods, Tools and Algorithms / R. Volkovičs // ENVIRONMENT. TECHNOLOGIES. RESOURCES: Proc. of the Int. Scientific and Practical Conf., 13 Jun. 2023. – Vol. 2. – P. 105–112.

29. El-Menshawy A., Gul Z., El-Thalji I. Azure machine learning studio and SCADA data for failure detection and prediction purposes: A case of wind turbine generator / A. El-Menshawy, Z. Gul, I. El-Thalji // IOP Conference Series: Materials Science and Engineering : Proc. of Conf., 1 Nov. 2021. – Vol. 1201, № 1. – Article 012086. – IOP Publishing.

30. Wang, J., Xu, C., Zhang, J., Zhong, R. Big data analytics for intelligent manufacturing systems: A review / J. Wang, C. Xu, J. Zhang, R. Zhong // Journal of Manufacturing Systems. – 2022. – Vol. 62. – P. 738–752.

31. Ward, B. Availability for Azure SQL / B. Ward // Azure SQL Revealed: A Guide to the Cloud for SQL Server Professionals. – 2021. – P. 373–439.

32. Franco, P., et al. IoT based approach for load monitoring and activity recognition in smart homes / P. Franco, et al. // IEEE Access. – 2021. – Vol. 9. – P. 45325–45339.

33. Akhmedova, Z. I. SQL (Structured Query Language) capabilities of the statistical database language / Z. I. Akhmedova // Multidisciplinary Journal of Science and Technology. – 2023. – Vol. 3, № 5. – P. 274–280.

34. Sarrab, M., Pulparambil, S., Awadalla, M. Development of an IoT based real-time traffic monitoring system for city governance / M. Sarrab, S. Pulparambil, M. Awadalla // Global Transitions. – 2020. – Vol. 2. – P. 230–245.

35. Mouha, R. A. R. Internet of Things (IoT) / R. A. R. Mouha // Journal of Data Analysis and Information Processing. – 2021. – Vol. 9, № 2. – P. 77.

36. Макєєв, О., Кравець, Н. Study of Methods of Creating Service-Oriented Software Systems in Azure / О. Макєєв, Н. Кравець // Computer Systems and Information Technologies. – 2023. – № 2. – С. 38–47.

37. Laghari, A. A., et al. A review and state of art of Internet of Things (IoT) / A. A. Laghari, et al. // Archives of Computational Methods in Engineering. – 2021. – P. 1–19.

38. Gupta, B. B., Quamara, M. An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols / B. B. Gupta, M. Quamara // Concurrency and Computation: Practice and Experience. – 2020. – Vol. 32, № 21. – Article e4946.

39. Zikria, Y. B., et al. Next-generation Internet of Things (IoT): Opportunities, challenges, and solutions / Y. B. Zikria, et al. // Sensors. – 2021. – Vol. 21, № 4. – Article 1174.

40. Nizetic, S., et al. Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future / S. Nizetic, et al. // Journal of Cleaner Production. – 2020. – Vol. 274. – P. 1–32.

41. Новіков, Ф. В., Новіков, Г. В., Жовтобрюх, В. О. Безпека життєдіяльності та інноваційні технології виробництва. – 2023.

42. de Almeida, M. G., Canedo, E. D. Authentication and authorization in microservices architecture: A systematic literature review / M. G. de Almeida, E. D. Canedo // Applied Sciences. – 2022. – Vol. 12, № 6. – Article 3023.

43. Moriarty, K., Farrell, S. Deprecating TLS 1.0 and TLS 1.1 / K. Moriarty, S. Farrell // Internet Engineering Task Force. – RFC 8996, 2021.

44. Черняк, О., та ін. Застосування функціональної залежності для багатокритеріального оцінювання безпеки праці, як об’єкта кваліметрії / О. Черняк, та ін. // Сучасний стан наукових досліджень та технологій в промисловості. – 2022. – Т. 1, № 19. – С. 76–84.

45. Шевченко, Є. Розробка кіберфізичної системи моніторингу технологічних процесів на виробництві / Є. Шевченко // Автоматизація та Приладобудування = Automation and Development of Electronic Devices (ADED'2023) : зб. студ. наук. ст. – Харків : ХНУРЕ, 2023. – Вип. 2. – С. 37–43.