IJARSCT
ISSN: 2581-9429
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Volume 5, Issue 4, April 2025
Impact Factor: 7.67

Azure Edge Computing: Enhancing IoT Deployments with Microsoft Azure

Praveen Borra[1], Mahidhar Mullapudi[2], Jhansi Xavier[3], Harshavardhan Nerella[4], Bheeshmachary Kommoju[5]
Computer Science, Florida Atlantic University, Boca Raton USA[1]
Senior Software Engineer, Microsoft USA[2]
Computer Science, Florida Atlantic University, Boca Raton USA[3]
Sr Cloud Engineer, Mass Mutual, USA[4]
Sr Manager of BI, Verizon Business, USA[5]
pborra2022@fau.edu, mahi.mullapudi@gmail.com , jxavier2023@fau.edu
nerellaharshavardhan@outlook.com, bheeshmacharykommoju@gmail.com

Abstract: *Edge computing has become indispensable in the landscape of the Internet of Things (IoT), enabling immediate data processing at or near the data source, thereby reducing latency and enhancing operational efficiency. Microsoft Azure stands out among cloud service providers by offering a comprehensive suite of tools specifically designed for deploying edge computing solutions. Leveraging Azure IoT services and Edge modules empowers organizations to extend their computing capabilities from centralized cloud environments to the edge of their networks.*

The integration of Azure's Edge computing capabilities into IoT deployments addresses several critical aspects essential for modern digital ecosystems. Primarily, it facilitates processing data closer to its origin, which proves beneficial in scenarios requiring rapid responses, such as industrial automation, remote monitoring, and smart cities. This proximity minimizes latency and optimizes overall system performance by reducing bandwidth usage.

Azure's versatile toolset supports a wide array of IoT applications, including predictive maintenance, anomaly detection, real-time analytics, and AI inferencing. These capabilities enable enterprises to derive actionable insights from data in near real-time, enhancing decision-making processes and operational agility.However, the adoption of Azure Edge computing presents challenges, particularly in managing edge devices distributed across various geographical locations. Robust security protocols, reliable connectivity solutions, and efficient device management strategies are crucial to ensure data integrity, scalability, and resilience.

In summary, Azure's Edge computing solutions represent a significant advancement in IoT deployments, empowering organizations to achieve higher levels of operational efficiency and intelligence. Azure's commitment to innovation and its ecosystem of Edge computing tools position it as a key facilitator of next-generation digital transformation initiatives globally.

Keywords: Cloud Computing, Microsoft Azure, Edge Computing, IoT, Azure IoT Hub, Azure IoT Edge, Azure Stack Edge, Azure IoT services, Latency reduction, Real-time analytics, Data processing, Edge modules

I. INTRODUCTION

The rapid proliferation of Internet of Things (IoT) devices has led to an unprecedented surge in data generation from diverse sources such as sensors, devices, and applications. This massive influx of data poses significant challenges in terms of processing, storing, and analyzing it efficiently. Traditional cloud computing models, while robust, often face limitations such as latency and bandwidth constraints, especially when dealing with real-time data processing needs.

DOI: 10.48175/IJARSCT-25155

Edge computing has emerged as a transformative solution to these challenges by decentralizing computational tasks. Unlike traditional cloud computing, where data is sent to centralized servers for processing, edge computing involves processing data closer to where it is generated—at the edge of the network. This approach reduces latency and optimizes bandwidth usage, crucial for applications requiring immediate response times and real-time decision-making [5].

Microsoft Azure has positioned itself as a leader in the field of edge computing, offering a comprehensive suite of tools designed to facilitate the deployment and management of edge computing solutions. Azure IoT Edge, for instance, extends Azure’s cloud intelligence to edge devices, enabling them to execute cloud workloads locally and respond swiftly to local events [6].

By leveraging Azure’s edge computing capabilities, organizations can enhance operational efficiency and reliability across their IoT ecosystems. For instance, industries such as manufacturing and healthcare can benefit from real-time analytics for predictive maintenance and patient monitoring, respectively. Azure’s edge solutions also prioritize security and compliance, addressing concerns around data privacy and regulatory requirements [6].Moreover, Azure enables organizations to harness advanced analytics, machine learning, and artificial intelligence models directly at the edge. This capability empowers businesses to derive deeper insights from IoT data, uncover hidden patterns, and optimize decision-making processes in near real-time [5].

In conclusion, Microsoft Azure’s advancements in edge computing technology represent a significant leap forward in enabling intelligent and responsive IoT ecosystems. By integrating cloud computing with edge capabilities, Azure not only enhances data processing efficiency but also accelerates digital transformation initiatives across various industries.

II. INTRODUCTION TO AZURE EDGE COMPUTING

Azure Edge computing extends Azure services to edge devices such as IoT devices, gateways, and nearby servers where data originates. This approach is pivotal in modern computing as it brings computational capabilities closer to data sources, thereby minimizing latency, optimizing bandwidth usage, and enhancing overall system reliability. This proximity to data sources is crucial for applications requiring real-time data processing and analysis, particularly in environments where continuous connectivity to the cloud may be limited or impractical.

Key components of Azure Edge computing include:

Azure IoT Hub

Azure IoT Hub serves as a centralized platform for managing secure connectivity and monitoring IoT devices [1]. It facilitates bi-directional communication between IoT devices and the cloud, ensuring secure and reliable data transmission.

Azure IoT Edge

This component enables the deployment of cloud workloads, AI models, and business logic directly onto IoT devices [2]. Azure IoT Edge extends Azure's cloud capabilities to the edge, allowing devices to perform local data processing, real-time analytics, and decision-making without relying solely on cloud resources.

Azure Stack Edge

Formerly known as Azure Data Box Edge, Azure Stack Edge integrates AI and IoT capabilities into edge devices for processing data locally [3]. It enables scenarios where real-time insights or immediate actions are required, even in disconnected or intermittently connected environments.

These Azure Edge computing solutions cater to various industry needs, including manufacturing, healthcare, retail, and smart cities, by enabling organizations to deploy scalable, secure, and responsive edge computing applications. By leveraging Azure's robust infrastructure and services, businesses can achieve operational efficiency, innovation, and improved customer experiences through timely data insights and actions.

DOI: 10.48175/IJARSCT-25155

III. AZURE IOT HUB

Azure IoT Hub is a pivotal component within Microsoft Azure's ecosystem, designed specifically to manage and facilitate secure communication between IoT devices and the cloud. As the foundational service for Azure's IoT solutions, Azure IoT Hub plays a critical role in enabling bi-directional communication between IoT devices and azure cloud services [1]. It ensures reliable and secure transfer of data, commands, and notifications at scale, making it essential for large-scale IoT deployments across various industries.In the realm of edge computing, Azure IoT Hub extends its functionality to the edge by facilitating the deployment of Azure IoT Edge [2]. This integration allows organizations to extend cloud intelligence and analytics to edge devices, such as gateways and local servers, where data is generated. By leveraging Azure IoT Edge, organizations can deploy and manage cloud workloads, AI models, and business logic directly onto IoT devices. This capability enables real-time data processing and analysis at the edge, reducing latency and optimizing bandwidth usage.

Moreover, Azure IoT Hub supports robust device management capabilities, including device provisioning, configuration, and monitoring [1]. This ensures that IoT devices connected to Azure IoT Hub are securely managed throughout their lifecycle, from initial deployment to ongoing operation. Security is paramount, with Azure IoT Hub providing built-in device-to-cloud and cloud-to-device communication encryption, device authentication, and access control mechanisms.This allows organizations to deploy Azure services closer to where data is generated, ensuring low-latency data processing and compliance with data residency requirements.

The Azure IoT Hub serves as a foundational service for managing IoT device connectivity and data ingestion securely into Azure. Its integration with Azure IoT Edgeempowers organizations to leverage edge computing effectively, enabling real-time analytics, reduced latency and enhanced operational efficiency at the edge.

IV. AZURE IOT EDGE

Azure IoT Edge enhances edge devices with cloud intelligence, enabling real-time data processing and AI inferencing directly at the source of data generation [2]. This capability is crucial in edge computing scenarios, where immediate processing near data sources reduces latency and enhances operational efficiency.Azure IoT Edge operates by deploying containerized workloads to edge devices, allowing seamless integration of cloud-based AI models, analytics, and IoT services [2]. Leveraging Docker containers and Kubernetes orchestration, Azure IoT Edge ensures scalable and efficient deployment across diverse edge environments.

Security is paramount in edge computing, and Azure IoT Edge offers robust mechanisms such as device-to-cloud and cloud-to-device communication encryption, role-based access control, and secure provisioning [2]. These features ensure data protection and compliance, essential for edge deployments in sensitive industries like healthcare and finance. Integration with Azure IoT Hub enables Azure IoT Edge to manage edge devices centrally from the cloud, facilitating monitoring, configuration, and software updates [1]. This integration ensures consistent operations and reliability across distributed edge environments.

The Azure IoT Edge runtime is integral for deploying custom and cloud-based logic directly on IoT Edge devices. Situated locally, this runtime manages critical operations such as workload installation and updates, adherence to Azure IoT Edge security standards, continuous module operation, and health reporting for remote monitoring through the cloud. It facilitates communication between downstream devices, inter-module interactions, and connectivity between IoT Edge devices and the cloud [9].

This runtime enables diverse deployment scenarios, commonly used for deploying AI to gateway devices that aggregate and process data from on-premises sources. Compatible with a wide range of IoT devices, it supports both Linux and Windows operating systems while abstracting hardware complexities. Devices vary from small, low-data processing units like those smaller than a Raspberry Pi 3, to robust industrial servers capable of handling intensive workloads [9].

The Azure IoT Edge plays a pivotal role in extending Azure's capabilities to edge devices, enabling real-time processing, AI inferencing, and secure operations directly at the edge. This enhances performance, reduces latency, and supports a wide range of applications and use cases across industries.

DOI: 10.48175/IJARSCT-25155

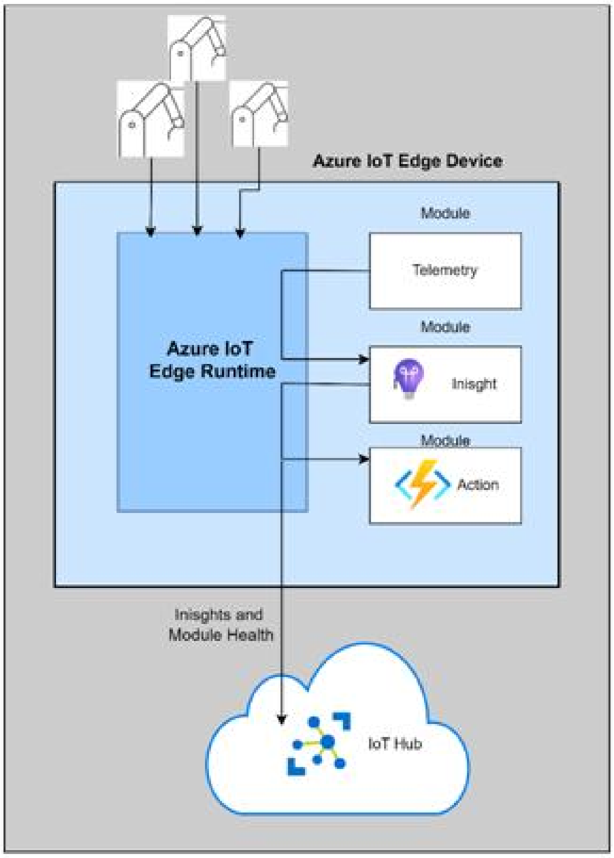


Figure 1: Azure IoT Edge runtime [9]

V. AZURE STACK EDGE

Azure Stack Edge is a critical component of Microsoft's edge computing portfolio, designed to empower organizations with AI and IoT capabilities directly at the edge of the network. This integration of compute, storage, and machine learning functionalities enables Azure Stack Edge to effectively process and analyze data locally, enhancing responsiveness and reducing latency [3].According to Microsoft [3], Azure Stack Edge facilitates the deployment of cloud workloads closer to where data is generated, whether in remote locations, manufacturing plants, or retail stores. This capability is crucial for applications requiring real-time data processing, such as video analytics, predictive maintenance, and autonomous systems.

Azure Stack Edge supports a hybrid cloud approach by extending Azure services to on-premises environments, ensuring consistency in application development and management across cloud and edge infrastructure [7]. This flexibility is beneficial for organizations needing to comply with data sovereignty regulations while leveraging the scalability and agility of the cloud.Security is a top priority for Azure Stack Edge, with Microsoft [3] highlighting built-in encryption, secure boot, and continuous monitoring features to protect data integrity and prevent unauthorized access. These robust security measures are essential for maintaining trust and compliance in edge computing environments.

Furthermore, Azure Stack Edge optimizes bandwidth usage by processing data locally and transmitting only relevant insights to the cloud, thereby reducing costs associated with data transfer and storage [7] This approach enhances operational efficiency and supports scalable deployment of edge computing solutions. The Azure Stack Edge integrates AI and IoT capabilities to enable efficient data processing at the edge, enhancing performance, security, and compliance for a wide range of edge computing applications.

DOI: 10.48175/IJARSCT-25155

VI. ADVANTAGES OF AZURE EDGE COMPUTING

Azure Edge Computing provides tailored advantages for IoT deployments, including minimized latency for real-time applications, optimized bandwidth usage, improved reliability amidst cloud connectivity disruptions, and enhanced data privacy through local processing of sensitive information [8]. These benefits collectively underscore Azure Edge Computing's effectiveness in supporting secure and efficient edge computing solutions.

- **Reduced Latency**: Azure Edge Computing achieves reduced latency by processing data locally at edge devices. This capability is critical for applications requiring instant responses and swift decision-making, as data doesn't need to travel to distant cloud servers and back.
- **Bandwidth Optimization**: By minimizing data sent to the cloud, Azure Edge Computing optimizes bandwidth utilization. This approach conserves network resources and reduces operational costs associated with data transmission and storage, making it ideal for IoT deployments where bandwidth constraints can be significant.
- **Enhanced Reliability**: Azure Edge Computing enhances application reliability by enabling edge devices to continue processing data locally during cloud connectivity disruptions. This ensures uninterrupted functionality and operational continuity even when cloud services are temporarily unavailable.
- **Data Privacy and Security**: Azure Edge Computing supports enhanced data privacy and security by processing sensitive information locally at the edge. This approach reduces the risk of data exposure during transmission over public networks and helps organizations comply with stringent data protection regulations.

VII. CHALLENGES AND CONSIDERATIONS IN AZURE EDGE COMPUTING

Implementing and managing Azure Edge solutions presents several distinct challenges that require careful consideration:

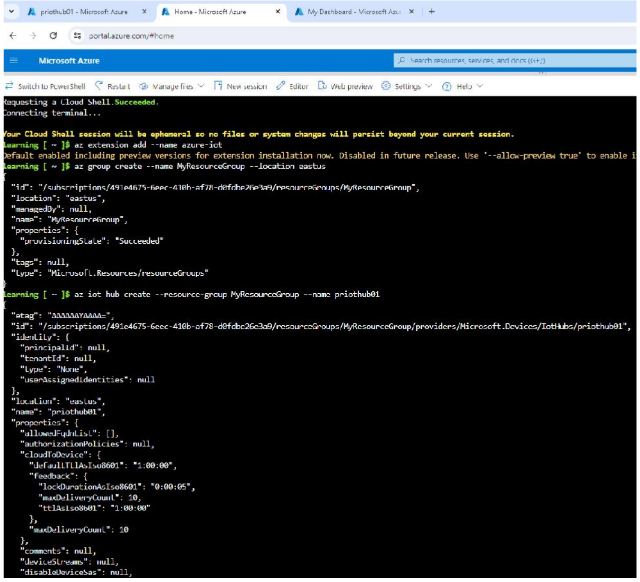
- **Complexity**: Effectively managing distributed edge environments demands specialized knowledge in networking and security protocols [1]. Coordinating various edge devices and ensuring seamless operation can be intricate, necessitating comprehensive management practices.
- **Scalability**: Ensuring consistent performance across diverse edge devices and locations poses significant scalability challenges [2]. Adapting to fluctuating workloads and demands while maintaining reliability requires meticulous planning and scalable architecture.
- **Integration**: Seamless integration of Azure Edge with existing IT infrastructures requires thorough planning and coordination. Compatibility, interoperability, and minimal disruption during deployment are crucial for successful integration and efficient operation.
- **Security**: Protecting edge devices from cybersecurity threats is critical to maintaining data integrity and operational continuity [4]. Implementing robust security measures such as encryption, access control, and device hardening is essential to mitigate risks associated with edge computing environments.

Addressing these challenges necessitates a holistic approach that combines technical expertise, strategic planning, and adherence to best practices in edge computing. By effectively managing complexity, ensuring scalability, facilitating seamless integration, and prioritizing robust security measures, organizations can optimize the benefits of Azure Edge Computing while mitigating potential risks.

VIII. METHODOLOGY

The Azure CLI was utilized to set up and manage an Azure IoT Hub. The following steps outline the process of creating the infrastructure and conducting the experiments [10]:

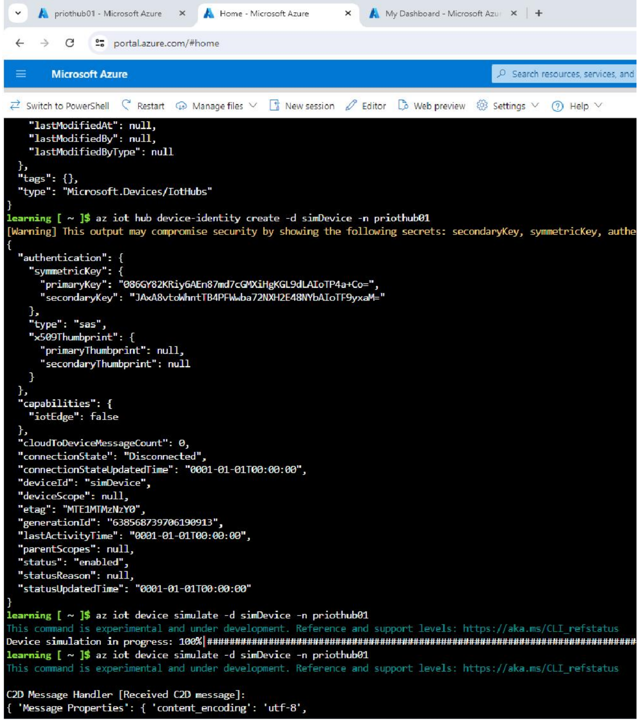
Creating the IoT Hub: The IoT hub was established using the Azure CLI, serving as the central point for device communication and telemetry ingestion.



```
Requesting a Cloud Shell.Succeeded.
Connecting terminal...

Your Cloud Shell session will be ephemeral so no files or system changes will persist beyond your current session.
learning [ ~ ]$ az extension add --name azure-iot
Default enabled including preview versions for extension installation now. Disabled in future release. Use '--allow-preview true' to enable i
learning [ ~ ]$ az group create --name MyResourceGroup --location eastus
{
  "id": "/subscriptions/491e4675-6eec-410b-af78-d0fdbe26e3a9/resourceGroups/MyResourceGroup",
  "location": "eastus",
  "managedBy": null,
  "name": "MyResourceGroup",
  "properties": {
    "provisioningState": "Succeeded"
  },
  "tags": null,
  "type": "Microsoft.Resources/resourceGroups"
}
learning [ ~ ]$ az iot hub create --resource-group MyResourceGroup --name priothub01
{
  "etag": "AAAAAAYAAAA=",
  "id": "/subscriptions/491e4675-6eec-410b-af78-d0fdbc26e3a9/resourceGroups/MyResourceGroup/providers/Microsoft.Devices/IotHubs/priothub01",
  "identity": {
    "principalId": null,
    "tenantId": null,
    "type": "None",
    "userAssignedIdentities": null
  },
  "location": "eastus",
  "name": "priothub01",
  "properties": {
    "allowedFqdnList": [],
    "authorizationPolicies": null,
    "cloudToDevice": {
      "defaultTtlAsIso8601": "1:00:00",
      "feedback": {
        "lockDurationAsIso8601": "0:00:05",
        "maxDeliveryCount": 10,
        "ttlAsIso8601": "1:00:00"
      },
      "maxDeliveryCount": 10
    },
    "comments": null,
    "deviceStreams": null,
    "disableDeviceSas": null,
```

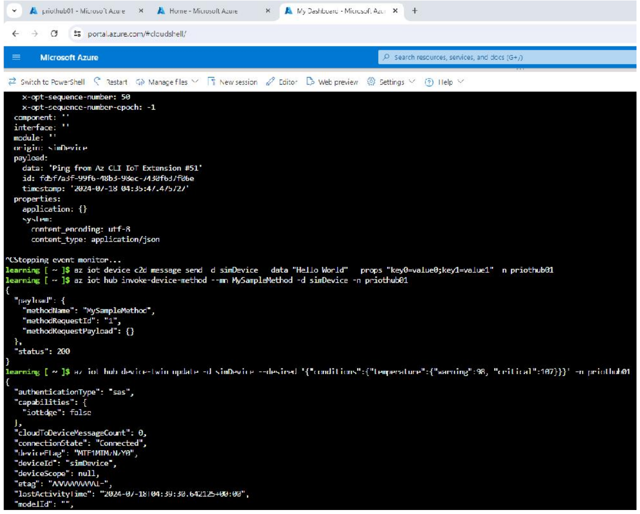
Setting Up a Simulated Device: A simulated device was created using the Azure CLI to generate and transmit telemetry data.



```
    "lastModifiedAt": null,
    "lastModifiedBy": null,
    "lastModifiedByType": null
  },
  "tags": {},
  "type": "Microsoft.Devices/IotHubs"
}
learning [ ~ ]$ az iot hub device-identity create -d simDevice -n priothub01
[Warning] This output may compromise security by showing the following secrets: secondaryKey, symmetricKey, authe
{
  "authentication": {
    "symmetricKey": {
      "primaryKey": "086GY82KRiy6AEn87md7cGMXiHgKGL9dLAIoTP4a+Co=",
      "secondaryKey": "JAxA8vtoWhntTB4PFWwba72NXH2E48NYbAIoTF9yxaM="
    },
    "type": "sas",
    "x509Thumbprint": {
      "primaryThumbprint": null,
      "secondaryThumbprint": null
    }
  },
  "capabilities": {
    "iotEdge": false
  },
  "cloudToDeviceMessageCount": 0,
  "connectionState": "Disconnected",
  "connectionStateUpdatedTime": "0001-01-01T00:00:00",
  "deviceId": "simDevice",
  "deviceScope": null,
  "etag": "MTE1MTMzNzY0",
  "generationId": "638568739706190913",
  "lastActivityTime": "0001-01-01T00:00:00",
  "parentScopes": null,
  "status": "enabled",
  "statusReason": null,
  "statusUpdatedTime": "0001-01-01T00:00:00"
}
learning [ ~ ]$ az iot device simulate -d simDevice -n priothub01
This command is experimental and under development. Reference and support levels: https://aka.ms/CLI_refstatus
Device simulation in progress: 100%|########################################################################
learning [ ~ ]$ az iot device simulate -d simDevice -n priothub01
This command is experimental and under development. Reference and support levels: https://aka.ms/CLI_refstatus

C2D Message Handler [Received C2D message]:
{ 'Message Properties': { 'content_encoding': 'utf-8',
```

Sending Telemetry: The simulated device was configured to send telemetry data, such as sensor readings and status updates, to the IoT hub.


priothub01 - Microsoft Azure
Home - Microsoft Azure
My Dashboard - Microsoft Azu
portal.azure.com/#cloudshell/
Microsoft Azure
Search resources, services, and docs (G+/)
Switch to PowerShell
Restart
Manage files
New session
Editor
Web preview
Settings
Help

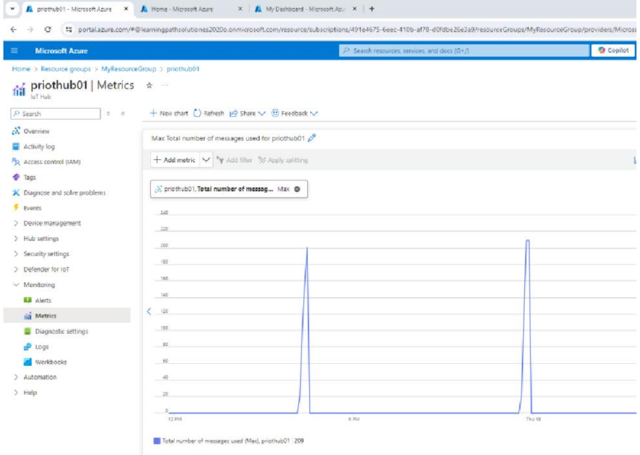
```
    x-opt-sequence-number: 50
    x-opt-sequence-number-epoch: -1
  component: ''
  interface: ''
  module: ''
  origin: simDevice
  payload:
    data: 'Ping from Az CLI IoT Extension #51'
    id: fdbf7a3f-99f6-48b3-98ec-7430f637f86e
    timestamp: '2024-07-18 04:35:47.475727'
  properties:
    application: {}
    system:
      content_encoding: utf-8
      content_type: application/json

^CStopping event monitor...
learning [ ~ ]$ az iot device c2d message send  d simDevice   data "Hello World"   props "key0=value0;key1=value1"  n priothub01
learning [ ~ ]$ az iot hub invoke-device-method --mn MySampleMethod -d simDevice -n priothub01
{
  "payload": {
    "methodName": "MySampleMethod",
    "methodRequestId": "1",
    "methodRequestPayload": {}
  },
  "status": 200
}
learning [ ~ ]$ az iot hub device-twin update -d simDevice --desired '{"conditions":{"temperature":{"warning":98, "critical":107}}}' -n priothub01
{
  "authenticationType": "sas",
  "capabilities": {
    "iotEdge": false
  },
  "cloudToDeviceMessageCount": 0,
  "connectionState": "Connected",
  "deviceEtag": "NTF1MTM/N/Y0",
  "deviceId": "simDevice",
  "deviceScope": null,
  "etag": "AAAAAAAAAAE=",
  "lastActivityTime": "2024-07-18T04:39:38.642125+00:00",
  "modelId": "",
```

Method Invocation: Methods were called on the simulated device through the Azure CLI, allowing for remote command execution.

Updating Desired Properties: Desired properties were set on the device to adjust its behavior and operational parameters.

Monitoring and Visualization: Device metrics and telemetry data were visualized using the Azure portal, offering real-time insights into the device's performance and data transmission.


priothub01 - Microsoft Azure
Home - Microsoft Azure
My Dashboard - Microsoft Azu
portal.azure.com/#@learningpathsolutions2020o.onmicrosoft.com/resource/subscriptions/491e4675-6eec-410b-af78-d0fdbe26e3a9/resourceGroups/MyResourceGroup/providers/Micros
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Resource groups > MyResourceGroup > priothub01
priothub01 | Metrics
IoT Hub
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Events
Device management
Hub settings
Security settings
Defender for IoT
Monitoring
Alerts
Metrics
Diagnostic settings
Logs
Workbooks
Automation
Help
New chart
Refresh
Share
Feedback
Max Total number of messages used for priothub01
Add metric
Add filter
Apply splitting
priothub01, Total number of messag... Max
240
220
200
180
160
140
120
100
80
60
40
20
0
12 PM
6 PM
Thu 18
Total number of messages used (Max), priothub01 209

IX. RESULTS

We successfully utilized Azure IoT Hub to handle high volumes of telemetry from IoT devices. The Azure CLI was employed to create both an IoT hub and a simulated device. Telemetry data from the simulated device was transmitted to the IoT hub, where we also performed additional operations including sending messages, invoking methods, and updating device properties. The Azure portal was then used to effectively visualize and monitor device metrics, showcasing the comprehensive capabilities of Azure IoT Hub in managing IoT device data.

X. CONCLUSION

In summary, Azure Edge Computing stands as a transformative technology in the realm of IoT and edge computing, offering tailored solutions for real-time data processing, enhanced reliability, optimized bandwidth usage, and strengthened data privacy and security. The benefits of reduced latency and improved application reliability highlight its suitability for critical applications demanding rapid responsiveness and uninterrupted operation. However, deploying Azure Edge solutions presents challenges such as managing complexity, ensuring scalability across diverse environments, seamless integration with existing IT infrastructure, and maintaining robust cybersecurity measures.

Effectively navigating these challenges requires a comprehensive approach that integrates technical expertise with strategic planning. This entails implementing rigorous management practices for distributed edge environments, adopting scalable architectures to accommodate varying workloads, orchestrating seamless integration with current systems, and prioritizing stringent security measures to protect against cyber threats.By addressing these considerations proactively, organizations can harness the full potential of Azure Edge Computing while mitigating potential risks. As the landscape of IoT and edge computing continues to evolve, Azure's capabilities position it as a leading solution for enabling secure, efficient, and resilient edge computing deployments that drive innovation and operational excellence across industries.

XI. FUTURE WORK

Future developments in Azure Edge Computing will emphasize advancing AI capabilities at the edge, refining edge-to-cloud orchestration, enhancing security and privacy protocols, ensuring scalability across varied environments, establishing interoperability standards, exploring applications in emerging technologies, and furthering edge analytics for predictive maintenance and operational efficiency in IoT contexts.

REFERENCES

[1]. Microsoft. Azure IoT Hub documentation. Accessed July 8, 2024, from https://docs.microsoft.com/en-us/azure/iot-hub/

[2]. Microsoft. Azure IoT Edge overview. Accessed July 8, 2024, from https://azure.microsoft.com/en-us/services/iot-edge/

[3]. Microsoft. Azure Stack Edge documentation. Accessed July 8, 2024, from https://docs.microsoft.com/en-us/azure/databox-online/data-box-edge-overview

[4]. Li, S., Da Xu, L., & Zhao, S. (2018). The internet of things: A survey. Information Systems Frontiers, 17(2), 243-259. doi:10.1007/s10796-014-9489-9

[5]. Satyanarayanan, M., et al. (2017). The Emergence of Edge Computing. IEEE Computer, 50(1), 30-39. doi:10.1109/MC.2017.9

[6]. Microsoft. Azure Documentation. Retrieved from https://azure.microsoft.com

[7]. Microsoft. Azure Stack Edge Security Documentation. Retrieved from https://docs.microsoft.com/en-us/azure/stack/edge/security/

[8]. Microsoft(2023). Azure Edge Computing Documentation. Retrieved from https://docs.microsoft.com/en-us/azure/edge-computing/

[9]. Microsoft. Azure IoT Edge. Microsoft Azure Documentation. Retrieved from https://learn.microsoft.com/en-us/azure/iot-edge/about-iot-edge?view=iotedge-1.5

[10]. Microsoft(2023). Azure IoT Hub Documentation. https://learn.microsoft.com/en-us/azure/iot-hub/quickstart-send-telemetry-cli

DOI: 10.48175/IJARSCT-25155