Edge Computing in Internet of Things

WHITEPAPER for SogetiLabs Circles

AMARJEET SINGH
MAHESH JADHAV

Index

1. Internet of Things 3
2. IoT Architecture on Cloud 4
3. Edge Device 5
4. Edge Computing IoT Architecture 6
5. Fog Computing 7
6. Securing IoT Architecture 9
7. Use Cases Built Using IoT Lambda Architecture 10
8. Summary 13

1. Internet of Things

Internet of Things i.e. IoT can be described as connected things or devices generating events and sending event messages for processing and generating actionable insights, which will be used to improve a business or process. In IoT connected devices can easily and securely interact with ingestion layer on cloud where this data is processed further to generate insights and actions or events to benefit a business process. Below figure shows the interaction between different parts of IoT platform.

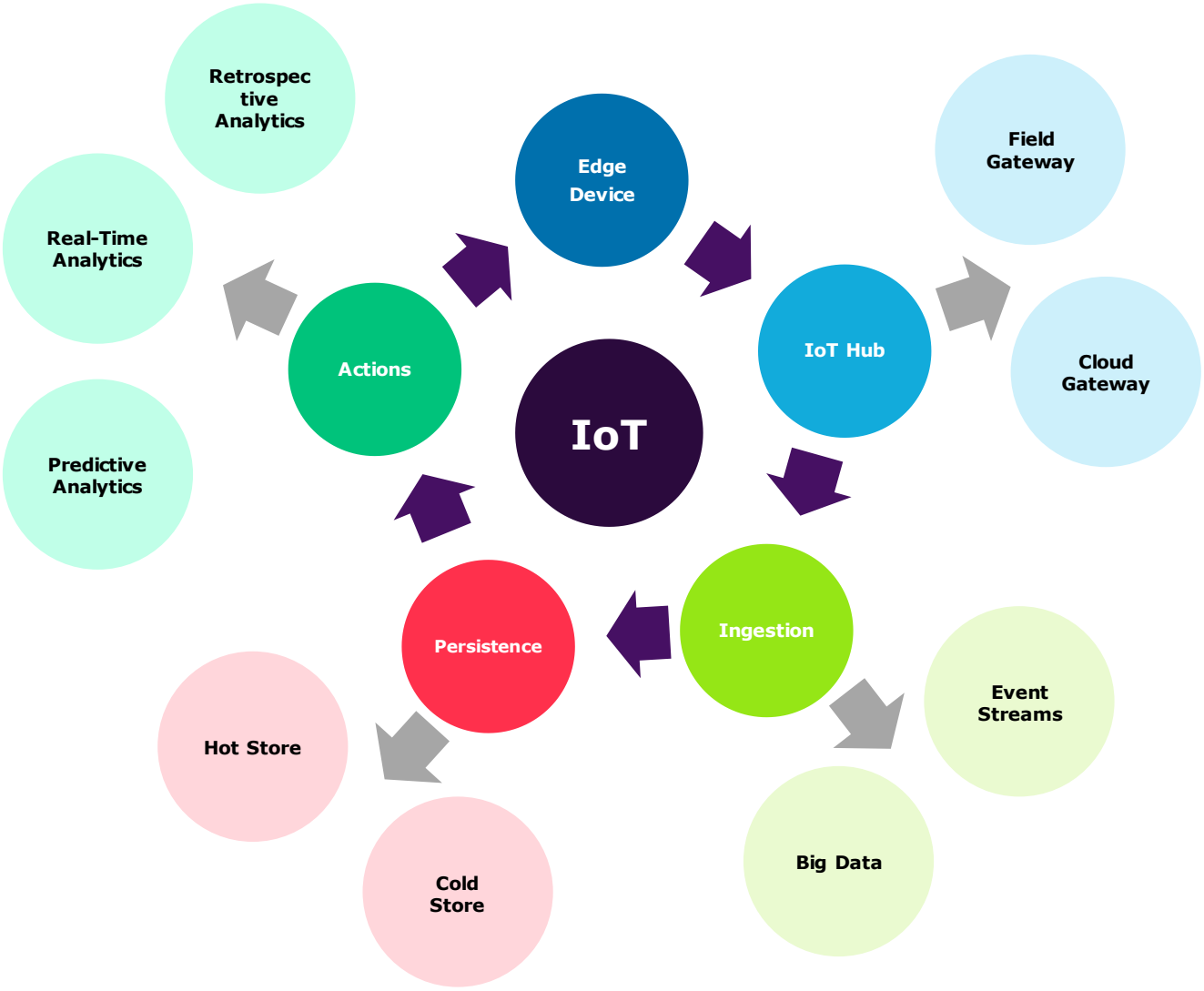

Figure 1: 1 Interaction between different parts of IoT

As we can see from Figure00201 above IoT has 5 main components.

It starts with the connected things; these connected things or devices could be basic devices collecting and sending data to IoT Hub or IoT Gateway on cloud. IoT Hub transfer data to Cloud platform which could be then analyzed through event streams and could be processed upon by pre-defined rules. The processed data and the raw data then can be persisted through persistence layer. This processed data is then used to create actions or events to improve the defined process, some events could be sent to devices to trigger action like switching off the device and switching on after some threshold is passed. So, the whole cycle keeps repeating and generating more and more volume of data which will be eventually used to make the process efficient and self-healing using technologies like Machine Learning and Deep Learning.

2. IoT Architecture on Cloud

Cloud platform provides shared services around IoT space which helps expediting the IoT implementation use cases. Once IoT use cases are implemented, it helps businesses capture the real-time events and avoid business losses by taking timely decisions. An ideal way to implement the IoT platform could be with the use of IoT Lambda Architecture and blue print as shown below:

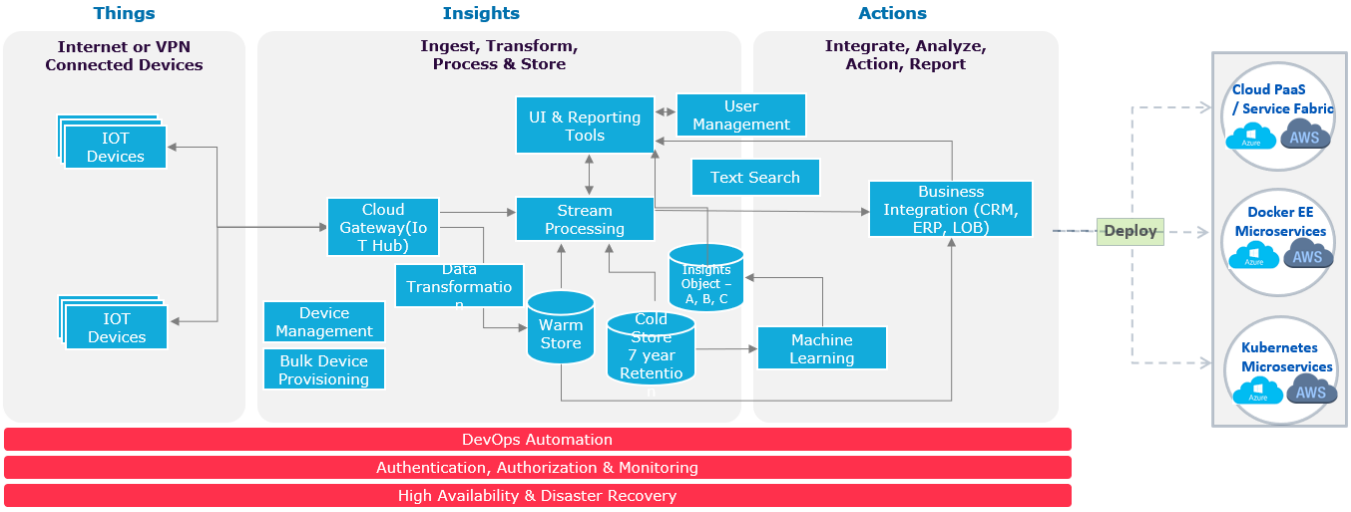

Figure 2: IoT lambda Architecture

Things include all the devices generating data, data collection logic near to devices and formating it in IoT communication protocol and ingesting it to cloud securely.

Insights consists data ingestion, transformation, processing and storing functions and services. It involve the cold and hot analytics path where hot path provides real time alarms and events around business critical functions of a system while cold path analysis mainly used for predictive as well as historical analysis.

Actions has components responsible for trigerring the actions addressed by action in the business process flow. Also it has insight interfaces to show visual representation of meaningful facts from data.

There is no doubt that IoT brings benefits to the business but over a period, due to huge amount of data ingestion and processing businesses comes across to below challenges:

- Increased cost of running these systems on cloud
- Data congestion on network due increase in data ingestion units
- Poor connectivity due to physical distance which results to latency
- Latency of response back results in missing on critical business events

If we must process and analyze this data, then we need a robust platform like cloud which is elastic and reliable to process and store this data. Edge computing comes very handy to mitigate the above-mentioned challenges for an IoT system.

3. Edge Device

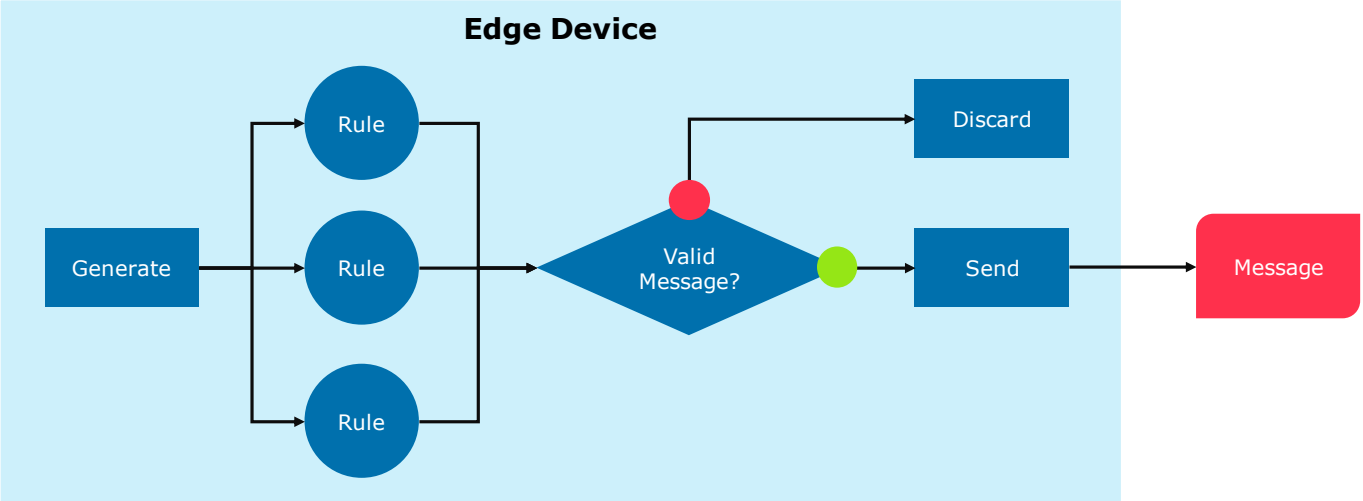

Figure 3: Edge compute device

Edge Device also called as Edge Compute Device, is the devices which has compute capabilities. As shown in Fig. 3 above, Edge devices has internal compute capability, it generates a message or an event which go through pre-defined rules which will evaluate the event and checks if the event is a valid event as per the rules, if not the event gets discarded at the device level itself else the event is then sent to IoT hub or gateway.

Traditional devices used to send the event as it is generated by the device, so there were too many unnecessary events also sent to the cloud for processing, this increases the data sent from device to cloud. To reduce the data to be sent to cloud and to minimize the processing complexity in the cloud we can make use of Edge devices which can discard the events at the local device level only.

Field gateways also can do the job of Edge devices, field gateways are local gateways which collects the data locally from several devices and then filter out the data to be sent to the cloud gateway or cloud IoT hub.

4. Edge Computing IoT Architecture

Edge computing IoT architecture as shown below is an extension to IoT and helps in processing data near to devices on the edge of network as shown below Edge connect introduced between devices and cloud gateway:

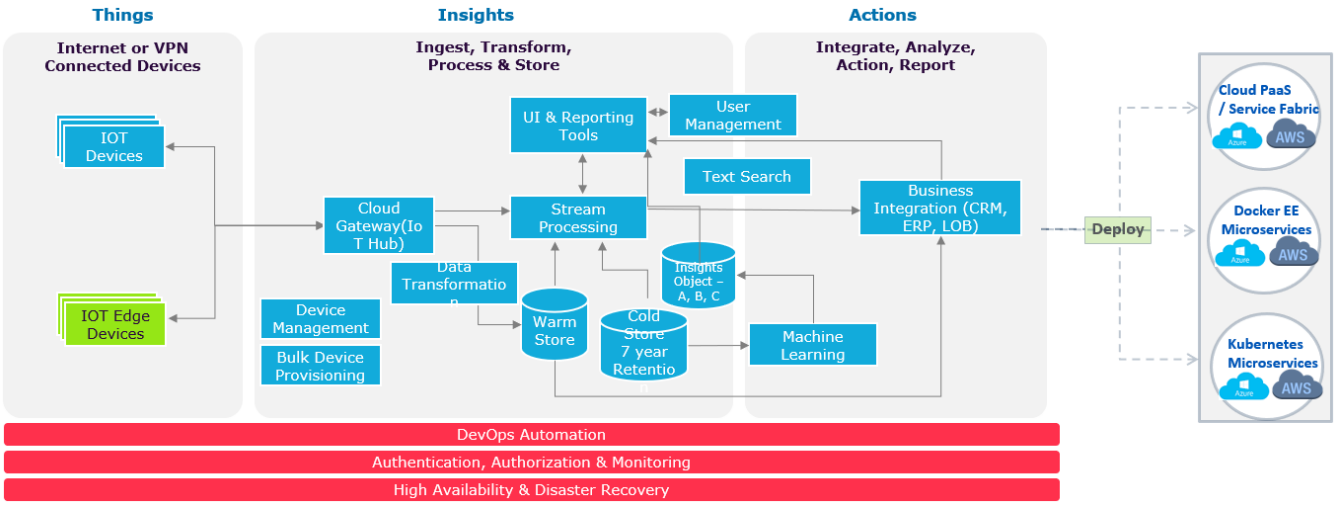

Figure 4: Edge computing IoT Architecture

As shown in the above diagram Edge Devices are processing units with increased compute power which has capability of processing and storing real time data near to the sensor devices and brings the below benefits to the business:

- Eliminates the single point of failure
- Reduce latency and improve response time
- Data is stored and processed on edge instead of transmitting to cloud platform
- Reduce the cost of transmitting and processing huge data on cloud

5. Fog Computing

As the edge computing market is growing and getting tractions, there is an important term related to edge that is catching on is fog computing. Fog refers to the network connections between edge devices and the cloud. Edge, on the other hand, refers more specifically to the computational processes being done close to the edge devices. So, fog includes edge computing, but fog would also incorporate the network needed to get processed data to its destination and adds one more block i.e. Edge connect to the IoT architecture as shown below:

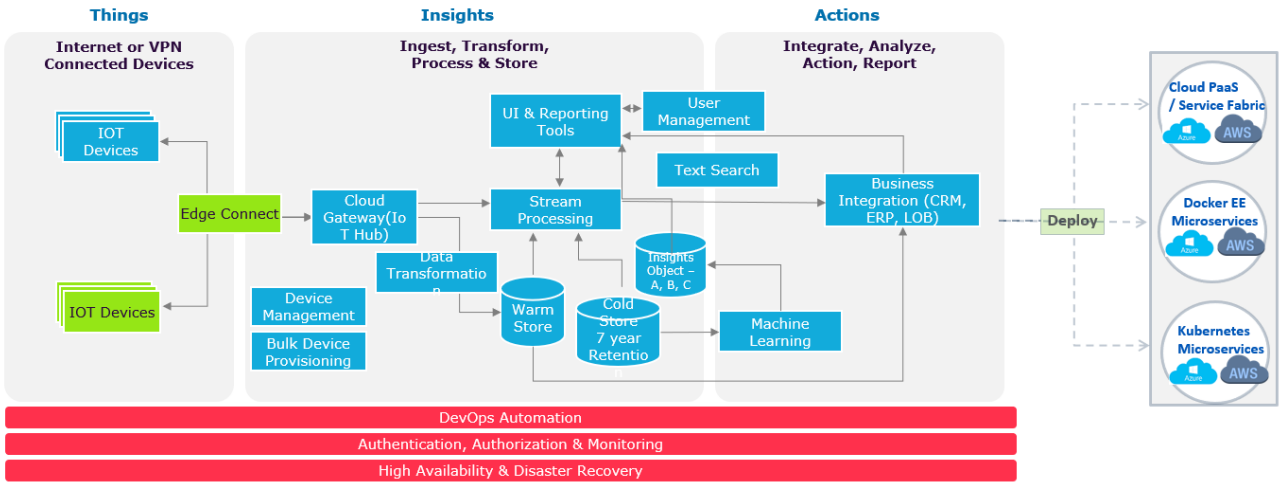

Figure 5: Edge Connect in Edge computing IoT Architecture

Security is one of the main concerns with IoT devices running on the edge of network because of their limited compute power and constraints of implementing security algorithms in it. Edge Connect block form the IoT architecture expanded below allows to implement different communication protocols and security algorithms as show below:

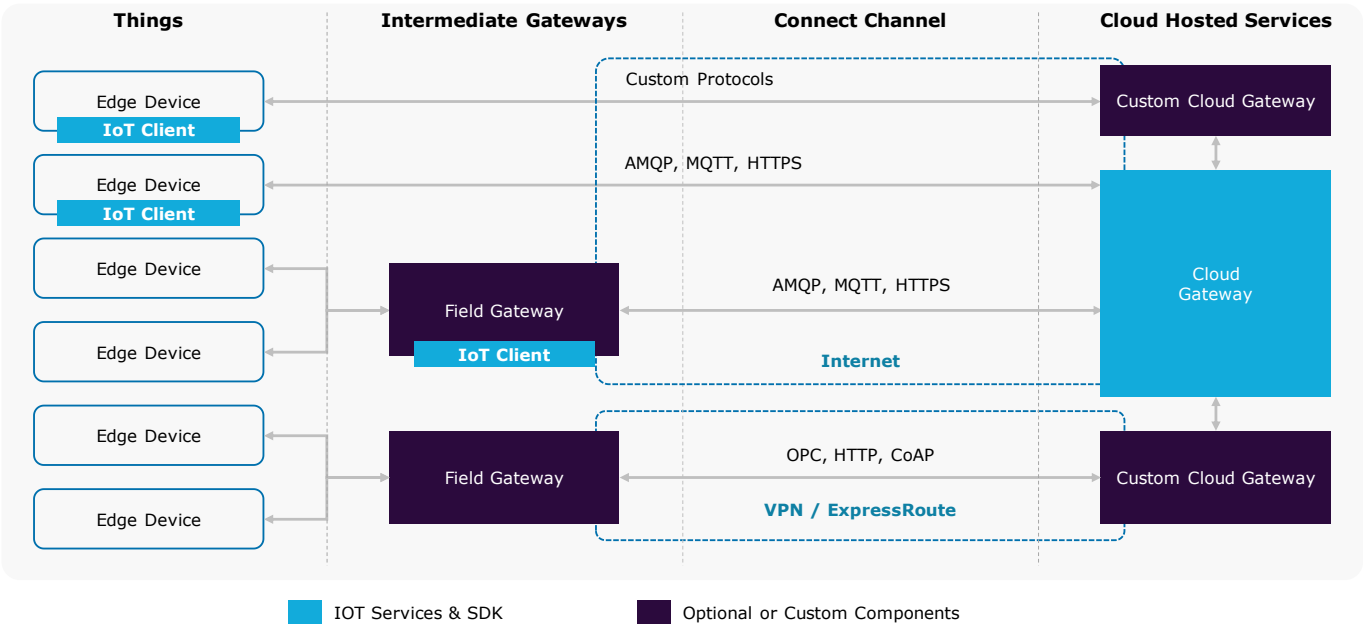

Figure 6: Edge Connect

Internet of Things communication protocols shown in the diagram are listed below:

- Hypertext Transfer Protocol (HTTPS)
- Advanced Message Queueing Protocol (AMQP)
- WebSocket protocol
- MQ Telemetry Transport (MQTT)
- Constrained Application Protocol (CoAP)
  - GSM short-message service (SMS)
  - The Open Mobile Alliance's (OMA)
  - Lightweight M2M protocol (LWM2M)
- OPC Unified Architecture (OPC UA) - Custom

6. Securing IoT Architecture

Identity access management to an IoT system is equally critical from security prospective to protect the data in transit & rest. As shown below, IoT system has option to authenticate & authorize through the active directory domains.

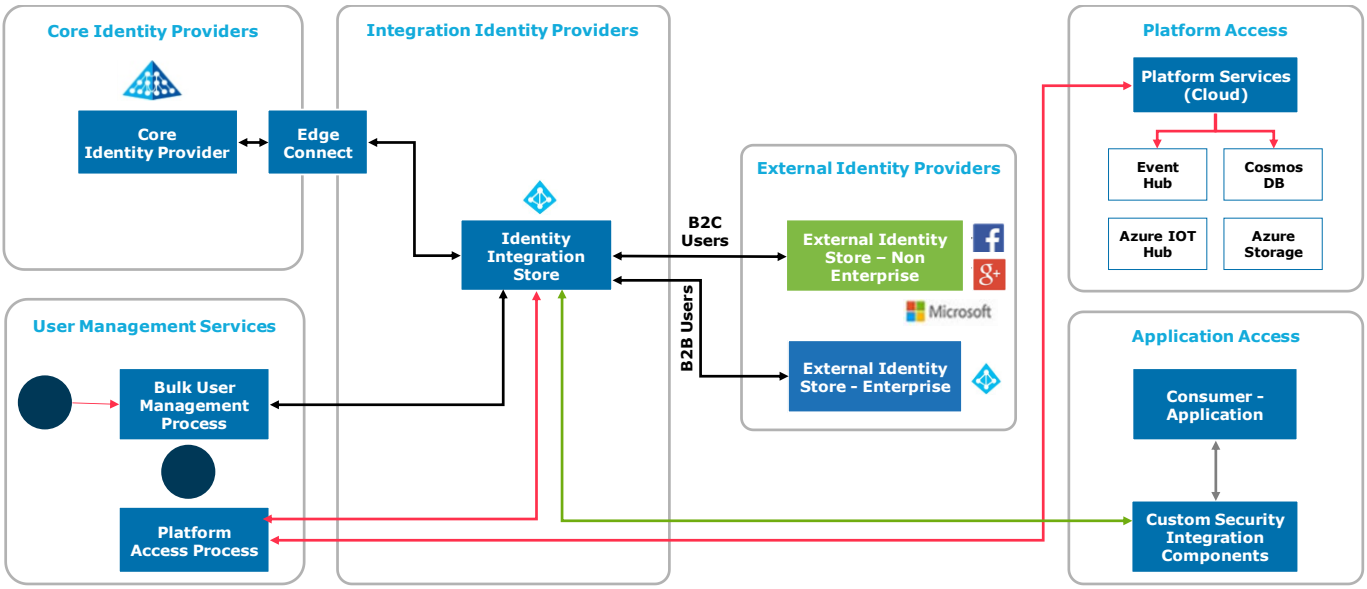

Figure 7: Identity Access Management in an IoT system

Implementation of the below mentioned features are shown in the above diagram:

- Bulk User Handling via Process using Files
- On premise Identity Provider, viz., AD, as core provider
- Cloud Hosted Integration Identity Provider, viz., AAD in B2B and/or B2C modes
- Sync with core Identity stores, viz. AD and AAD
- RBAC based User access for Cloud platform services
- Role based User access to applications
- Monitor & Self-Healing

7. Use Cases Built Using IoT Lambda Architecture

Plant Growth Monitoring

Use Case Name

Crop growth monitoring and management through connected edge computing devices helps users to check real time and historical effects on various crops according to the treatments provided.

Description

Users can also use predictive model to predict the plant growth according to provided data.

Using real time data analytics, users can take appropriate actions like killing or removing the crop.

Various dashboards are provided to users for real time, historical and predictive and logs management.

To monitor AWS cloud activities all logs will be collected and filtered to show log monitor dashboard using ELK tool.

Beneficiaries:

Farmers, Agriculture, Genomics

System Diagram

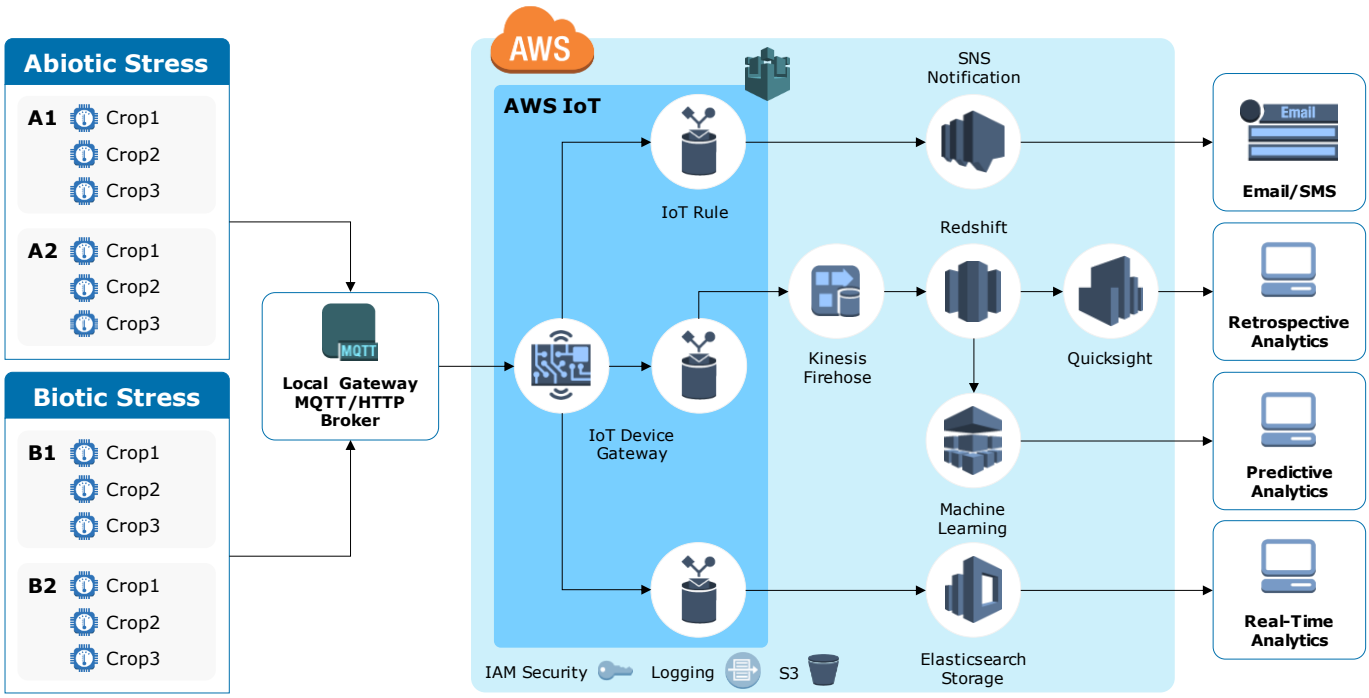

Figure 8: System Diagram

Events

In this proposed design, 3 different types of crops, like rice, corn and soybean, will undergo 4 different types of treatments A1, A2, B1 and B2. This treatment is categorized into 2 parts Abiotic stress (A1, A2) like temperature, humidity and Biotic stress (B1, B2) like insects, virus etc.

Each plant will have sensor device which will collect data having temp, humidity, plant height, plant leaves count etc. metrics and send it to in-field or local field gateway using MQTT protocol.

This local field gateway will aggregate around 100 items and send it to AWS IoT hub using MQTT, MQTT handles intermittent connection between Device and AWS Cloud.

AWS IoT will have a Big Data backend which will process, store and analyze the data to show 4 different kinds of data analytics –

Real time analytics – user can see plant growth in near real time

Historical or retrospective analytics – user can see reports of last 1 month or year

Predictive analytics- user can predict the data

Log analytics – user can monitor AWS access and issues

Facial Recognition

Use Case Name

Using Azure cognitive services like Computer Vision and Face which can do image processing, list the happiest faces with ranks from the group of people.

Description

Several images of a group of people will be taken by a camera, processing will be done on this image using Azure cognitive services which will provide the happiest face from the group and show the first three happy faces on the dashboard. The dashboard will also display the IoT events analysis data.

System Diagram

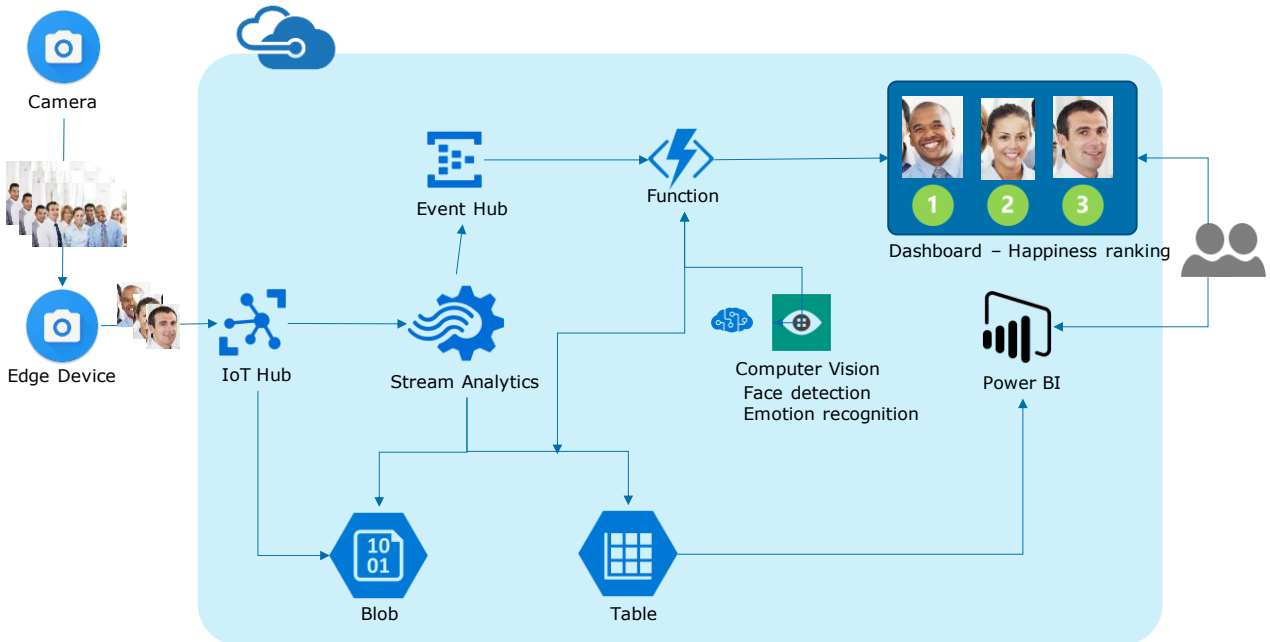

Figure 9: Facial Recognition

Events

1. Camera will take continuous images of group of people, atleast 20-30 per minute.
2. These images will be provided to Azure IoT Hub
3. This stream of data is provided to stream analytics processing which will be stored in a Blob storage, also metadata of the image will also be stored in azure table
4. Stream analytics will send an event to event hub with id in table
5. Event hub will pass the id to Azure function which will get the image from blob from the table id image link, and will pass the image to Azure Cognitive Services – Face api to process the image.
6. Face API will use below 2 main APIs
   i. Face Detection api
   ii. Emotion Detection api
7. Output of computer vision api will be store in Azure Table with all related data
8. Power BI will be used to show dashboard for IoT events using Azure Table as its source
9. We may need to create a simple webapp to show the happiest faces with ranks from the group

8. Summary

In this way IoT Lambda Architecture combines IoT and Edge computing together to mitigate the latency and response time for IoT systems and devices. It also reduces the security challenges and helps in bringing the cloud operational cost down due to reduced storage requirements and data volume processing to achieve the meaningful insights out of data.

About Sogeti

Sogeti is a leading provider of technology and engineering services. Sogeti delivers solutions that enable digital transformation and offers cutting-edge expertise in Cloud, Cybersecurity, Digital Manufacturing, Digital Assurance & Testing, and emerging technologies. Sogeti combines agility and speed of implementation with strong technology supplier partnerships, world class methodologies and its global delivery model, Rightshore®. Sogeti brings together more than 25,000 professionals in 15 countries, based in over 100 locations in Europe, USA and India. Sogeti is a wholly-owned subsidiary of Capgemini SE, listed on the Paris Stock Exchange.

Learn more about us at www.sogeti.com