REFERENCE ARCHITECTURE

Securing Edge to Cloud IoT Solutions with Intel and Amazon Web Services

Intel®-based IoT Gateways
AWS IoT Services
Internet of Things

Steve Paper
Intel Corporation

Kris Keppens
Intel Corporation

Andrew John
Intel Corporation

Claudiu Pasa
Amazon Web Services

The Internet of Things (IoT) is at the heart of a powerful technology revolution. The act of connecting devices and systems to each other so that they can share data, is the seed of new products, services, and experiences. IoT provides companies with greater insight into how customers are using and interacting with their products by collecting the valuable data these devices and systems produce.

AWS and Intel have collaborated to offer a joint reference architecture that provides a foundation for seamlessly and securely connecting devices and delivering trusted data to the cloud to create new value through analytics.

Companies and organizations have been collecting and storing data for years. Now, new data analytics technologies increases the value of this data through by extracting meaningful information. This information leads to smarter decision making that drives tangible business outcomes.

However, building an end-to-end IoT solution is a challenging task for many customers. There are a lot of components to consider, including; devices and sensors at the edge, communication protocols, cloud infrastructure, business applications that make use of IoT data, management systems, deployment, monitoring, and maintenance. When developing an IoT system, it's important that customers make choices that lead to a solution that works not just as a prototype, but also scales to production level in a secure and manageable way.

The IoT platform developed in collaboration between AWS and Intel

The solution begins at the edge, where security starts at the silicon layer with Intel®-based IoT gateways and an ecosystem of compatible sensors and devices. These hardware devices include software built with AWS Greengrass and the AWS IoT Device SDK to securely connect them to AWS IoT and ultimately, AWS endpoints such as Amazon DynamoDB, AWS Lambda, and other big data and analytics services. From there, customers and partners can build software to connect any number of devices with the full breadth and depth of AWS services to build or integrate vertical specific IoT applications while gaining value through data analytics.

“By using AWS cloud services, companies are able to build agile solutions that can scale to meet tremendous device growth…while building on top of secure cloud computing infrastructure.”

Intel IoT Platform

The Intel IoT Platform includes an end-to-end reference architecture and a family of products from Intel and its ecosystem as a foundation for securely connecting devices, and delivering trusted data to the cloud.

This solution scales from the development phase of an IoT implementation into production by leveraging Intel’s ecosystem of Original Device Manufacturers (ODMs) that build IoT Gateways pre-configured with AWS Greengrass to execute and update solution logic on devices. Further, Intel®-based IoT gateways can be fully managed and through device registration and management services from the Wind River® Helix™ Device Cloud. When combined with AWS services, Intel Reference hardware enables customers to quickly develop and deploy IoT systems. When it is time to go into production, customers can work with ODMs to manufacture the exact hardware they need for their use case, have automatically register hardware with AWS IoT on the factory floor, roll-out solution logic across their device fleet, and remotely manage device OS updates, reboots, and configuration changes with Device Cloud.

This document will describe features and capabilities of Intel®-based IoT gateway hardware, Device Cloud, AWS IoT, and AWS Greengrass, and how they can be combined to build complete IoT solutions in the cloud for customers.

IoT & AWS

One of the value propositions of an Internet of Things (IoT) strategy is the ability to provide insight into context previously invisible to business decision makers. Part of developing an IoT strategy is selecting a platform that meets the foundational principles of an IoT solution.

AWS defines the Internet of Things according to three pillars: Intelligence, Cloud Orchestration and Things. Customers of all sizes and across multiple sectors are committing to a connected future. Your connected devices generate volumes of data that provide the intelligence needed for organizations like yours to make better, faster decisions. Adopting IoT solutions allows you to gain actionable insights from your device data, which quickens the pace of innovation so you can create new business models, expand existing operations and improve efficiencies.

Connected devices will create the largest source of data ever. This data will come from billions of devices and applications, will come in multiple forms and will need to be stored, queried, combined and analyzed to provide new insights into businesses that were previously unknown. These insights form the basis of intelligence in which the real value lies. First step is to connect your devices. For that, you need cloud orchestration.

Cloud orchestration is key to simplifying IoT solutions. To connect and manage millions, sometimes, billions of devices, requires an agile, scalable, secure, and cost-effective cloud platform on which to store and ingest data, communicate between devices and users, build applications and manage IoT solutions. Customers can integrate their IoT practice with AWS services like AWS Lambda, Device Shadows, Amazon DynamoDB, Amazon EC2 and more. These components, together, are the core capabilities of an IoT platform that form the foundation AWS IoT. The true value of the IoT comes from the intelligence gained through extracting insights from data generated from devices and then applying business logic to gain domain knowledge from which actions follow either automated or manual. With effective cloud orchestration from AWS IoT, customers securely and scalably connect devices, make sense of their data, and build applications and new business models.

If you knew the state of everything and could reason on that knowledge, what problems would you solve?

The Core Tenets of IoT

- **Agility** – The freedom to quickly analyze, execute, and build business and technical initiatives in an unfettered fashion.
- **Scale** – Seamlessly expand infrastructure regionally or globally to meet operational demands.
- **Cost** – Understand and control the costs of operating an IoT platform.
- **Security** – Secure communication from device through cloud while maintaining compliance and iterating rapidly.

By using AWS cloud services, companies are able to build agile solutions that can scale to meet tremendous device growth, with an ability to manage cost, while building on top of secure cloud computing infrastructure.

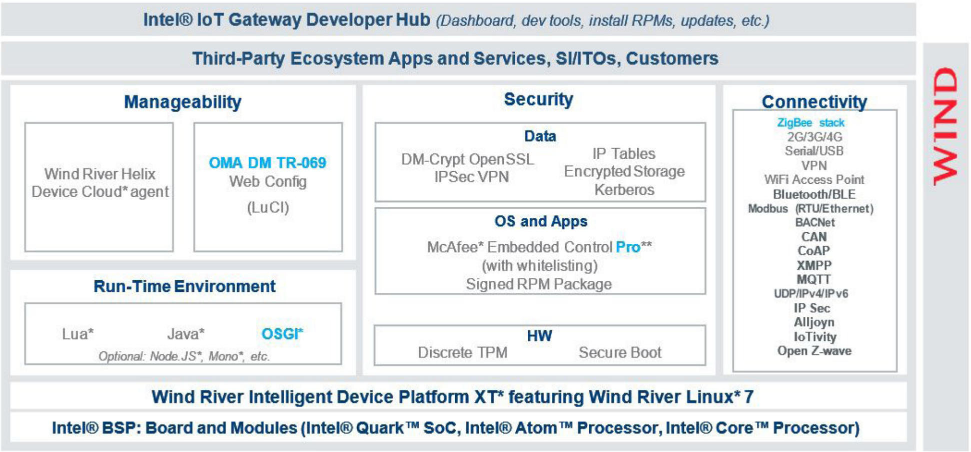
Companies that select a platform that offer these core benefits and promotes them to the market will improve organizational focus on the differentiators of its business and the strategic value of implementing solutions that leverage the Internet of Things.

AWS IoT

AWS IoT is a managed cloud platform that lets connected devices easily and securely interact with cloud applications and other devices. AWS IoT can support billions of devices and trillions of messages, and can process and route those messages to AWS endpoints and to other devices reliably and securely. With AWS IoT, your applications can keep track of and communicate with all your devices, all the time, even when they aren't connected.

With AWS IoT, it easy to use AWS services like AWS Lambda, Amazon Kinesis, Amazon S3, Amazon Machine Learning, Amazon DynamoDB, and many others, to build IoT applications that gather, process, analyze, and act on data generated by connected devices, without having to manage any infrastructure.

AWS IoT supports HTTP, WebSocket, and MQTT, a lightweight communication protocol specifically designed to tolerate intermittent connections, minimize the code footprint on devices, and reduce network bandwidth requirements. It also supports other industry-



Intel® IoT Gateway Developer Hub *(Dashboard, dev tools, install RPMs, updates, etc.)*

Third-Party Ecosystem Apps and Services, SI/ITOs, Customers

Manageability

Wind River Helix Device Cloud* agent

OMA DM TR-069
Web Config
(LuCI)

Run-Time Environment

Lua* Java* OSGI*

Optional: Node.JS, Mono*, etc.*

Security

Data

DM-Crypt OpenSSL
IPSec VPN

IP Tables
Encrypted Storage
Kerberos

OS and Apps

McAfee* Embedded Control Pro**
(with whitelisting)
Signed RPM Package

HW

Discrete TPM Secure Boot

Connectivity

ZigBee stack
2G/3G/4G
Serial/USB
VPN
WiFi Access Point
Bluetooth/BLE
Modbus (RTU/Ethernet)
BACNet
CAN
CoAP
XMPP
MQTT
UDP/IPv4/IPv6
IP Sec
Alljoyn
IoTivity
Open Z-wave

Wind River Intelligent Device Platform XT* featuring Wind River Linux* 7

Intel® BSP: Board and Modules (Intel® Quark™ SoC, Intel® Atom™ Processor, Intel® Core™ Processor)

All products, dates, and figures specified are preliminary based on current expectations, and are subject to change without notice.
*Other names and brands may be claimed as the property of others. **This includes whitelisting, change control & read/write permissions
[1]Requires purchase of third-party hardware,

> *“With AWS IoT, you can filter, transform, and act upon device data on the fly, based on business rules you define.”*

standard and custom protocols, and devices can communicate with each other even if they are using different protocols.

Authentication and end-to-end encryption throughout all points of connection help the AWS IoT service to make sure data is never exchanged between devices and the service without proven identity. In addition, you can secure access to your devices and applications by applying policies with granular permissions.

With AWS IoT, you can filter, transform, and act upon device data on the fly, based on business rules you define. You can update your rules to implement new device and application features at any time.

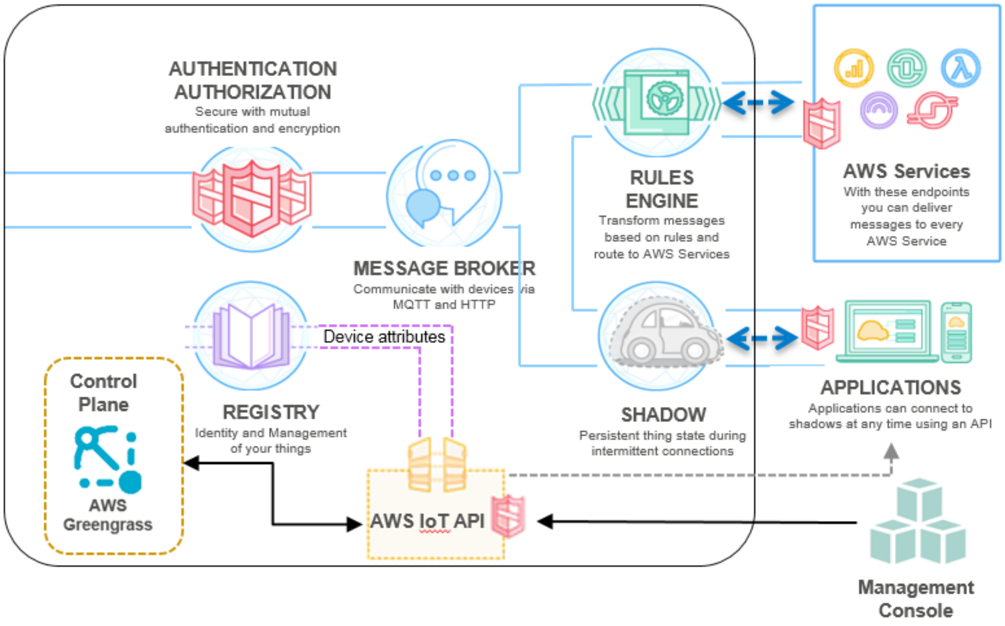
Using Device Shadows, AWS IoT stores the latest state of a device so that it can be read or set at any time, making the device in the cloud appear to your applications as if it were online all the time. This means that your application can read a device’s state even when it is disconnected, and also allows you to set a device state and have it implemented when the device reconnects.

AWS Greengrass

AWS Greengrass is software that extends AWS Lambda and AWS IoT onto devices. Greengrass takes advantage of your devices’ onboard capabilities, and extends to the cloud for management, updates, and elastic compute and storage. AWS Greengrass brings familiar languages and programming models from the cloud to local devices. Developers create and test device software in the cloud, and then deploy that software to local devices using a managed service. With AWS Greengrass, devices can act locally on the data they generate, while still using the cloud for management, analytics, and durable storage.

Some core capabilities of AWS Greengrass are:

- **Local AWS Lambda** — Execution of Lambda serverless compute functions locally on the device meaning your code executes in response to local events without need of transit latency, even when a device is not connected to the Internet.
- **Local Messaging** — Messaging between devices on a local network, so they can communicate with each other as part of a cohesive, distributed solution even


AUTHENTICATION
AUTHORIZATION
Secure with mutual authentication and encryption
MESSAGE BROKER
Communicate with devices via MQTT and HTTP
RULES ENGINE
Transform messages based on rules and route to AWS Services
AWS Services
With these endpoints you can deliver messages to every AWS Service
REGISTRY
Identity and Management of your things
Device attributes
SHADOW
Persistent thing state during intermittent connections
APPLICATIONS
Applications can connect to shadows at any time using an API
Control Plane
AWS Greengrass
AWS IoT API
Management Console

"AWS IoT leverages an event-driven architecture and works with other AWS Services for application development, storage, analytics and visualization."

when there is no connection to AWS.

- **Local Device Shadows** — The ability to cache device data locally and track the current vs. desired state of devices, reduces the amount of raw data which needs transmission to the cloud so you can achieve rich insight at a lower cost.

Almost any device with a general-purpose CPU can host Greengrass Core, which includes the full functionality. OEMs can create dedicated appliances to host Greengrass Core for added storage, compute, or redundancy. In addition, simple microcontroller-based constrained devices can use the AWS IoT Device SDK to interact with Greengrass Core on other devices.

Reference Architecture Components and Integration

This section defines the components and integration framework comprising of Intel IoT platform and Amazon Web Services.

Secure Communications
Like AWS IoT, AWS Greengrass authenticates and encrypts device data at all points of connection, so that data is never exchanged between devices and the cloud without proven identity. Greengrass uses the same security and access management customers are familiar with in AWS, with mutual device authentication and authorization, and secure connectivity to AWS IoT.

The AWS IoT reference architectures outline the key components and how customers can leverage Intel and AWS IoT offerings to build secure end-to-end IoT solutions.

Intel Edge Components

- Wind River Linux: is the leading commercial embedded Linux platform hardened for IoT
- Intel Hardware Security: Secures the platform at the hardware level with capabilities such as secure boot, Intel Trusted Execution Technology.
- Intel Processors: Provides unique performance scalability across Intel Quark SoC, Atom, Core and Xeon processor families.
- Wind River Pulsar Linux: is a small-footprint commercial grade binary Linux OS based on the Wind River Linux distribution that connects seamlessly to Wind River Helix Cloud.
- Wind River Intelligent Device Platform XT: Simplifies the development, integration, and deployment of IoT gateways with a customizable middleware development environment.
- McAfee Integrity Control: Performs monitoring, management, and tight security policy enforcement on edge devices.

Intel Device Management and Security

- Wind River® Helix™ Device Cloud: Provides device management services (device monitoring, device control, software updates), device registration, device attestation, and secure deployment at scale. Device Cloud leverages McAfee ePolicy Orchestrator to ease administration of distributed devices, automate security policy control, and simplify compliance reporting.

AWS IoT Data Ingestion

AWS IoT is a managed cloud-based service for Internet of Things devices, that currently includes an IoT Device SDK, Registry, Device Shadows, Rules Engine and Authentication & Authorization services. AWS IoT leverages an event-driven architecture and works with other AWS Services for application development, storage, analytics and visualization.

"The IoT solution collaboratively developed by AWS and Intel enables a wide range of solutions that let customers use IoT and data analytics to drive tangible outcomes from connected edge devices, no matter where those devices are located."

AWS IoT currently consists of the following components:

Message Broker — Provides a secure mechanism for devices and IoT applications to publish and receive messages from each other. You can use the MQTT protocol to publish and subscribe. In addition, you can use the HTTP REST interface to publish.

Rules Engine — Provides message processing and integration with other AWS services. You can use a SQL-based language to select data from message payloads, process the data, and send the data to other services, such as Amazon S3, Amazon DynamoDB, and AWS Lambda. You can also use the message broker to republish messages to other subscribers.

Thing Registry — Sometimes referred to as the Device Registry. Organizes the resources associated with each device. You register your devices and associate up to three custom attributes with each device. You can also associate certificates and MQTT client IDs with each device to improve your ability to manage and troubleshoot your devices.

Thing Shadows Service — Provides persistent representations of your devices on the AWS Cloud. You can publish updated state information to a Thing Shadow, and your thing can synchronize its state when it connects. Your things can also publish their current state to a Thing Shadow for use by applications or devices.

Thing Shadow — Sometimes referred to as a Device Shadow. A JSON document used to store and retrieve current state information for a thing (device, app, and so on).

Device Gateway — Enables devices to securely and efficiently communicate with AWS IoT.

Security and Identity Service — Provides shared responsibility for security on the AWS Cloud. by keeping your things' credentials safe in order to send data securely to the message broker. The message broker and rules engine use AWS security features to send data securely to devices or other AWS services.

Work Flow and Usage Models

AWS and Intel collaborated to create a differentiated IoT architectural framework that enables security and scalability from edge to cloud, speeds deployment and helps customers gain business insights while realizing operational cost savings. The IoT solution collaboratively developed by AWS and Intel enables a wide range of solutions that let customers use IoT and data analytics to drive tangible outcomes from connected edge devices, no matter where those devices are located.

With the tremendous growth of intelligent devices, security is a primary concern for IoT solution deployment that needs to be addressed. Secure Intel hardware and software solutions paired with AWS' mutual authentication security model help customers connect things to the cloud, integrate those devices with existing infrastructure, and securely manage data. Because the Intel®-based IoT gateways come pre-configured and application-ready, customers can quickly take advantage of IoT solutions to increase efficiency, reduce costs, and solve business problems. Intel®-based IoT gateways also enable seamless and secure data flow between edge devices and the AWS Cloud through pre-integrated, pre-validated hardware and software building blocks. Customers' IoT solutions can then deliver valuable business insights based on data from connected devices at the network edge.

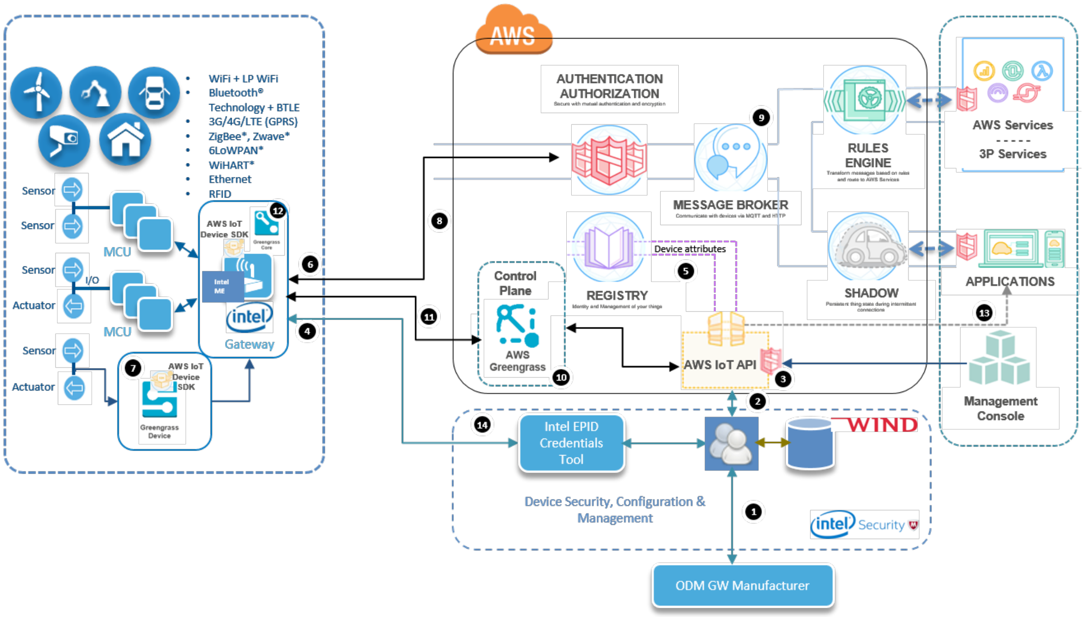
Deployment Experience

The IoT solution collaboratively developed by AWS and Intel has been designed to deliver secure zero-touch onboarding of gateways with hardware root of trust.

Let's walk through a typical IoT deployment scenario: As devices are deployed in the field, it is important to track the device inventory data as a list of gateways (regardless of the ODM manufacturer), their serial number, MAC address and certificates. As part of this architecture, this device inventory data is securely ingested into the Wind River® Helix™ Device Cloud at the factory floor of the ODM manufacturer through DXL (Data Exchange Layer-) based bulk provisioning APIs. This device inventory is made available to AWS IoT and backend CRM applications via secure APIs exposed by Device Cloud. It can also be synced up with the help of business logic and workflows on AWS IoT or backend CRM applications such as those that perform automatic periodic updates or nightly refreshed background jobs. The devices are shipped to customer location(s) and upon powering up at the customer site, the gateway device securely boots up and is attested by Device Cloud, based on hardware root of trust. Upon successful registration, Device Cloud automatically inserts the certificates into the device. The AWS Greengrass SDK or custom code leveraging the AWS IoT SDKs use the Intel Management Engine (ME) APIs to retrieve the device certificates. The stand-alone application or Greengrass Core on the Intel®-based IoT gateway establishes a secure data channel using MQTT or WebSocket protocols to AWS IoT using the AWS certificate authentication mechanism. The Greengrass deployment receives device communication configuration and the Intel IoT Gateway gets device configuration from Device Cloud. Leveraging one or both of these sources of configuration, the gateway connects to the sensors and sensor modules. Once the secure data channel is established, stand-alone applications or Lambda functions deployed in a Greengrass Core on the gateway receive sensor data and start processing and transmitting data to and receiving data from the AWS IoT platform. All these steps are automated, creating a seamless deployment experience requiring minimal intervention by the end customer.

Deployment, Registration, Authentication

1. ODM initiates Gateway provisioning by sending device inventory data (list of Gateways, serial number, certs) to



"All these steps are automated, creating a seamless deployment experience requiring minimal intervention by the customer."

Device Cloud. Device Cloud ingests device inventory data securely through REST APIs

2. AWS IoT Hub gets device inventory data via Device Cloud APIs
3. Provisioning Applications takes care of provisioning subscriptions
4. Once customer powers ON the Gateway, the device securely boots up and Device Cloud attests the Gateway
5. Device Cloud inserts device certificates into AWS device registry via APIs
6. AWS agent authenticates with AWS IoT Hub using device certificates on the GW (Hardware Root of Trust) and establishes secure data path to the cloud

Telemetry, Data Ingestion

7. Business Applications on the devices acquires data from connected sensors
8. AWS IoT Client inside AWS Greengrass on the Gateway transmits sourced data up to AWS IoT
9. Data messages are routed, processed, stored and made available for enterprise integration

Device Management and SW Updates

10. AWS Greengrass Service packages device configuration and Lambda functions that are a part of the overall IoT solution
11. AWS Greengrass Service then performs an over-the-air update to deploy the package from the AWS Cloud to one or many Greengrass Cores
12. The Greengrass Core gracefully updates the configuration and locally operating Lambda functions to reflect the new package
13. Application Software Manager pushes the updates to Device Cloud using APIs
14. Device Cloud prepares signed RPM packages and pushes themit securely to the Gateway
15. The Intel agent on the gateway upgrades the Software

Summary

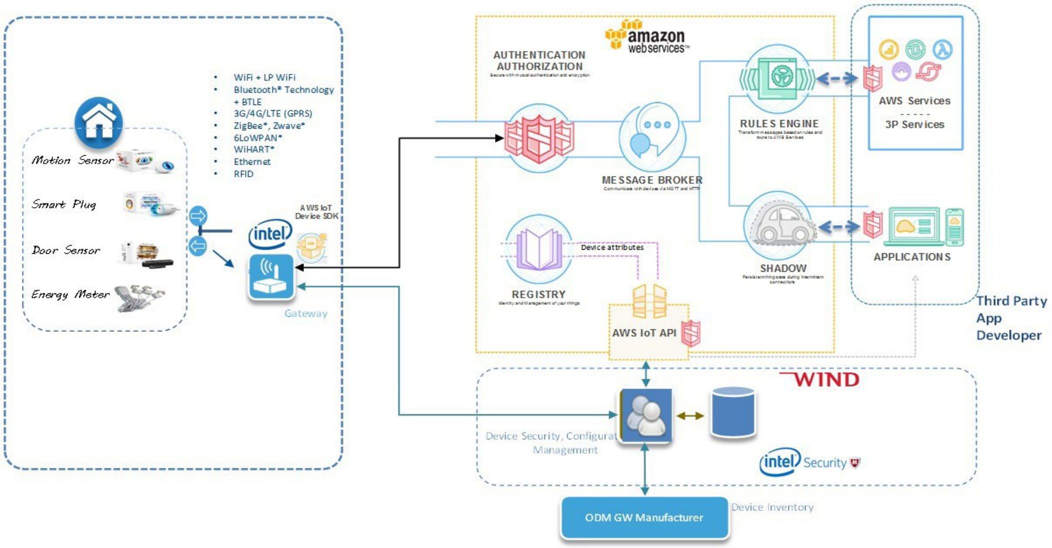
The IoT solution collaboratively developed by AWS and Intel provides a compelling architecture for IoT, and provides tools and products for connecting the "unconnected", unlocking the value of and visualizing data, then monetizing the insights that data contains. While the Intel IoT Platform provides the foundation for connecting devices, with security and manageability, AWS IoT and AWS Greengrass enable you to connect devices to AWS services and to other devices, securely process and act upon device data, and enable local and remote applications to interact with devices even when they are offline.

AWS and Intel solutions can help customers take advantage of IoT to uncover inefficiencies, reduce risk and cost, seize new opportunities, obtain business insights, and increase revenue. More than a million businesses worldwide already trust AWS. Now, through IoT solutions powered by the Intel, companies can revolutionize their relationships with customers through new capabilities made possible by real time connected data.

Use Case

Energy Monitoring & Home Safety

AWS and Intel collaborated to develop a Smart Home platform to deliver energy monitoring, home safety and surveillance services. Utility companies that generate and distribute power can offer these services to their end customers leveraging this platform. The Intel IoT Gateway platform connects to multiple sensors such as smart energy meters/clamps, power plugs, door locks, window sensors, IP cameras, and more. In addition, Device Cloud provides device security and management capabilities. Sensor data is aggregated at the Gateway and sent to the AWS Cloud over IP/Cellular connection. Then, AWS IoT provides data ingestion, storage, and analytics capabilities. Smart Home applications for energy monitoring, home safety, and surveillance both on the cloud and gateway device can be provided by a 3rd party application vendor that can develop and launch cloud applications on AWS IoT platform as well device applications on the Intel®-based IoT gateway.


Motion Sensor
Smart Plug
Door Sensor
Energy Meter
WiFi + LP WiFi
Bluetooth® Technology + BTLE
3G/4G/LTE (GPRS)
ZigBee*, Zwave*
6LoWPAN*
WiHART*
Ethernet
RFID
AWS IoT Device SDK
intel
Gateway
amazon web services™
AUTHENTICATION AUTHORIZATION
Secure with mutual authentication and encryption
MESSAGE BROKER
Communicate with devices via MQTT and HTTP
RULES ENGINE
Transform messages based on rules and route to AWS Services
SHADOW
Persistent thing state during intermittent connections
REGISTRY
Identity and Management of your things
Device attributes
AWS IoT API
AWS Services
3P Services
APPLICATIONS
Third Party App Developer
WIND
Device Security, Configurat Management
intel Security
ODM GW Manufacturer
Device Inventory

Technology Components Function	
Sensors	Door Sensors, Smart Plugs, Energy Meters, IP Cameras, Thermostats, Smart Bulbs
Intelligent Gateway	• Seamless connectivity to Sensors (via Zigbee, Zwave, BLE, 802.11) • WAN Connectivity to the Cloud (via 3G, LTE, Ethernet, Wi-Fi) • Filtering and Aggregation of data at the Edge • Home Apps for Energy Monitoring and Management, Home • Safety, Home Surveillance (offline mode) • Secure Connection to the AWS Cloud via AWS Device SDK
AWS IoT Platform	Data Ingestion, Storage
Wind River® Helix™ Device Cloud	Device Management, Registration, & Attestation
Cloud Applications	• Customer Apps build on AWS • Dashboard, Visualization, Reports • Energy Monitoring and Management • Home Safety & Surveillance Applications

These services will not only improve customer retention, but also enable new revenue generating opportunities for Utility companies.

Connected Mine & Predictive Maintenance
AWS and Intel collaborated to develop a Connected Mine platform that delivers asset tracking and predictive maintenance solutions. Mining companies need to operate expensive equipment under harsh conditions. One of their key challenges is extending the life of high-value assets such as haul trucks and other mining equipment. This requires collecting high-frequency, high-resolution data from these assets as well as positional data under challenging conditions and network constraints. The Intel IoT Gateway platform connects to multiple sensors that collect data on vehicle location, IMU, strut pressure, oil leak sensors, and more. The IoT gateway has multiple network connections such as WiFi, 3G/4G/LTE and LoRa and can switch between network connections depending on the conditions. Data can be ingested locally at GW running AWS Greengrass Core, and the sensor data is aggregated and filtered at the gateway. This allows the gateway to be operated in "offline" mode when network conditions are constrained and data cannot be efficiently transmitted to the cloud. The AWS Greengrass Core stack can also run edge analytics facilitating real-time processing of data and analytics on-site, without suffering the network availability and latency constraints of processing data in the cloud. AWS Greengrass connects to the AWS IoT platform and syncs up with relevant data as necessary when network bandwidth is available. The data collected is used to create road roughness models and detect abnormal track conditions and take corrective action. This corrective action allows smoother operations and less wear and tear of high-value assets. The Wind River® Helix™ Device Cloud provides device security and remote management capabilities.

Technology Components Function	
Sensors	GPS/Location, IMU (Inertial Measurement Unit), Strut Pressure, Oil Leak
Intel IoT Gateway	• Seamless connectivity to Sensors (via Zigbee, Zwave, BLE, 802.11) • WAN Connectivity to the Cloud (via 3G, LTE, Ethernet, Wi-Fi) • Filtering and aggregation of data at the Edge • Home Apps for Energy Monitoring and Management, Home • Safety, Home Surveillance (offline mode) • Secure connection to the cloud via AWS Greengrass
AWS Greengrass	Local data ingestion, storage, analytics
AWS IoT Platform	Cloud data ingestion, storage, analytics
Wind River® Helix™ Device Cloud	Device management, registration, & attestation
Cloud Applications	• Customer Apps build on AWS • Dashboard, Visualization, Reports • Road Roughness Models • Predictive Maintenance • Home Safety & Surveillance Applications

Technical Appendices

Appendix A: Sensors

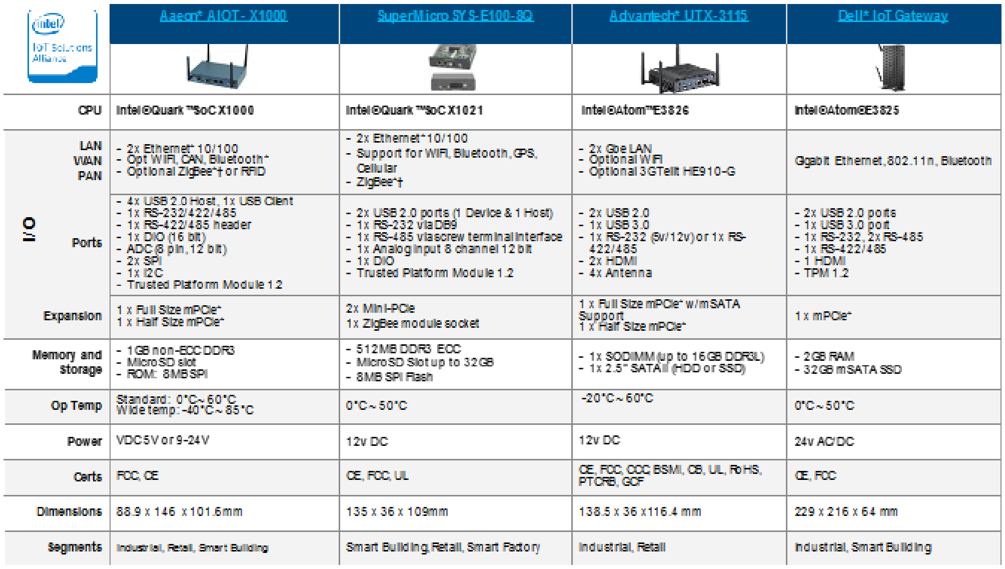
To get started, here is a representative list of sensors that are interoperable with Intel®-based IoT gateways.

Intel has a vibrant ecosystem of 3rd party partners, who are members are of the Intel IoT Solutions Alliance, and provide hundreds of sensors that are interoperable with the IoT Gateway. Intel has developed a strategy of providing a robust number of sensors that are applicable to a variety of use cases and business solutions; the strategy has been developed leveraging sensors that have been directly validated by Intel and through leveraging Intel's partner ecosystem to pull through the sensors that they have validated by leveraging their middleware solutions.

Sensor Type	Part Number	Protocol	Vertical	Interface
Occupancy and daylight harvesting	Aura Interior	BACNet	Smart Building	RS485
Energy Meter	Veris E50H5	BACNet	Smart Building	RS485
Modbus 3 Phase Energy Meter	Veris H8035-0100-2	Modbus RTU	Smart Building	RS485
Wall Mount Temp	Veris HWXPHTX	Modbus RTU	Smart Building	RS485
Humidity	Veris HD2XMSTA1	Wire	Smart Building	GPIO
Temp	Comet T0310	Modbus RTU	Industrial	RS232
Temp/Humidity	Comet T3311	Modbus RTU	Industrial	RS232
Temp/Humidity	Omega RH-USB	Basic Serial	Industrial	USB
Open Z-Wave	Various (400+ devices)	Z-Wave	Smart Home	USB or RS232
Interface to Phillips Hue Bridge	Hue Bulbs and Lamps	ZigBee	Smart Home	IP

Appendix B: IoT Gateways

Here is a representative list of IoT gateways manufactured by Intel's ODM ecosystem. For a broader list of IoT gateways, please refer to the Intel IoT Solutions Alliance.



		Aaeon* AIOT- X1000	SuperMicro SYS-E100-8Q	Advantech* UTX-3115	Dell* IoT Gateway
	CPU	Intel®Quark™SoC X1000	Intel®Quark™SoC X1021	Intel®Atom™E3826	Intel®Atom®E3825
I/O	LAN WAN PAN	- 2x Ethernet* 10/100 - Opt WIFI, CAN, Bluetooth* - Optional ZigBee*† or RFID	- 2x Ethernet* 10/100 - Support for WIFI, Bluetooth, GPS, Cellular - ZigBee*†	- 2x Gbe LAN - Optional WIFI - Optional 3GTelit HE910-G	Gigabit Ethernet, 802.11n, Bluetooth
	Ports	- 4x USB 2.0 Host, 1x USB Client - 1x RS-232/422/485 - 1x RS-422/485 header - 1x DIO (16 bit) - ADC (8 pin, 12 bit) - 2x SPI - 1x I2C - Trusted Platform Module 1.2	- 2x USB 2.0 ports (1 Device & 1 Host) - 1x RS-232 via DB9 - 1x RS-485 via screw terminal interface - 1x Analog Input 8 channel 12 bit - 1x DIO - Trusted Platform Module 1.2	- 2x USB 2.0 - 1x USB 3.0 - 1x RS-232 (5v/12v) or 1x RS-422/485 - 2x HDMI - 4x Antenna	- 2x USB 2.0 ports - 1x USB 3.0 port - 1x RS-232, 2x RS-485 - 1x RS-422/485 - 1 HDMI - TPM 1.2
	Expansion	1 x Full Size mPCIe* 1 x Half Size mPCIe*	2x Mini-PCIe 1x ZigBee module socket	1 x Full Size mPCIe* w/mSATA Support 1 x Half Size mPCIe*	1 x mPCIe*
	Memory and storage	- 1GB non-ECC DDR3 - MicroSD slot - ROM: 8MB SPI	- 512MB DDR3 ECC - MicroSD Slot up to 32GB - 8MB SPI Flash	- 1x SODIMM (up to 16GB DDR3L) - 1x 2.5" SATAII (HDD or SSD)	- 2GB RAM - 32GB mSATA SSD
	Op Temp	Standard: 0°C~60°C Wide temp: -40°C~85°C	0°C~50°C	-20°C~60°C	0°C~50°C
	Power	VDC 5V or 9-24V	12v DC	12v DC	24v AC/DC
	Certs	FCC, CE	CE, FCC, UL	CE, FCC, CCC, BSMI, CB, UL, RoHS, PTCRB, GCF	CE, FCC
	Dimensions	88.9 x 146 x 101.6mm	135 x 36 x 109mm	138.5 x 36 x 116.4 mm	229 x 216 x 64 mm
	Segments	Industrial, Retail, Smart Building	Smart Building, Retail, Smart Factory	Industrial, Retail	Industrial, Smart Building