EQST insight

주요 Cloud IoT Native 서비스 현황 및 이용 시 고려해야 하는 보안 사항

AI·Cloud·Data·IoT 등 지능형 기술이 지속적으로 발전하면서, 많은 양의 데이터 처리 및 활용을 위해 Cloud와 IoT 환경은 점점 밀접한 관계를 가지게 될 것이다. 이에 따라 발생하는 보안의 필요성에 대해 고찰해 보고자 한다.

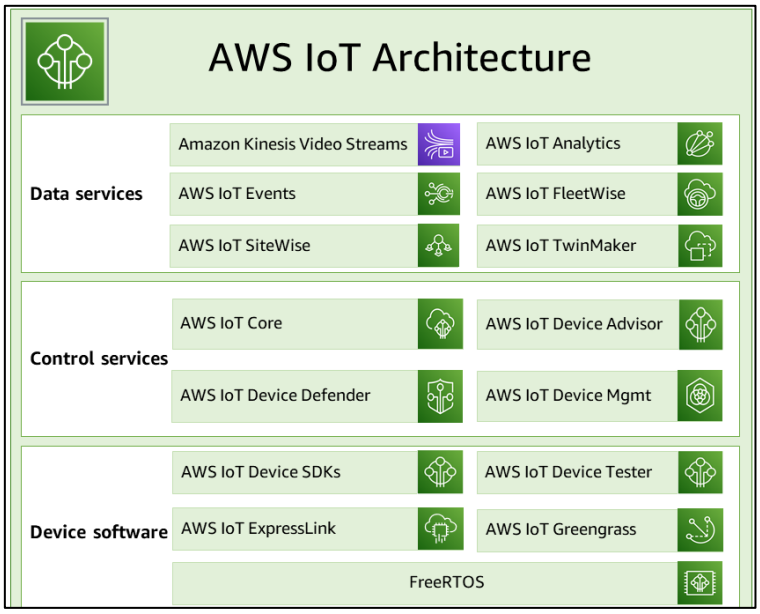
1. Cloud IoT Native 서비스 현황 및 개요

현재 국내·외의 여러 CSP(Cloud Service Provider)들은 Cloud 서비스 및 리소스 사용 시 안전한 이용을 위해 비즈니스 또는 개인 환경에서 다양한 형태의 보안 솔루션, Native 서비스, 보안 설정, 옵션 등을 지원하고 있다. IoT 영역 또한 기기 연결, 관리, 분석, 개발을 위한 다양한 Cloud Native 서비스들을 제공하고 있다.

Cloud와 IoT 영역이 점차 확장, 성장함에 따라 여러 Cloud 관련 보안 취약점이 발견되거나 사고가 발생하고 있어 보안의 중요성이 점점 커지고 있다. 이번 EQST insight 헤드라인에서는 IoT 분야와 Cloud 환경 사이에서 Cloud Native 서비스 이용 시 보안 고려 사항을 기술하며, 대표적인 클라우드 공급업체인 AWS, Azure, GCP 3사의 Cloud IoT에 대한 간략한 설명 및 보안 관련 insight를 작성했다.

1) AWS (Amazon Web Services)

AWS IoT는 IoT 기기 연결을 위한 Cloud 서비스와 관리, 분석 등을 위한 서비스를 제공하며, IoT 서비스를 3개 영역(디바이스 소프트웨어, 제어 서비스, 데이터 서비스) 15개 서비스로 구분하고 있다.



[AWS IoT 아키텍처 ①]

각 영역 및 세부 서비스에 대해 자세히 살펴보면 다음과 같다.

a. 디바이스 소프트웨어 영역

디바이스 소프트웨어 영역은 사용자의 IoT 디바이스를 지원하기 위한 소프트웨어를 제공해 개발 및 배포 등의 확장성을 지원해 주는 영역으로 상세 서비스는 다음과 같다.

infosec

서비스 명	설명
AWS IoT Device SDK	샘플 개발자 및 포팅 안내서를 포함하고 있어 사용자가 하드웨어 플랫폼에 따라 IoT 제품 또는 솔루션을 손쉽게 구축할 수 있도록 지원해 주는 서비스
AWS IoT Device Tester	마이크로 컨트롤러용 테스트 자동화 도구로서 디바이스가 AWS IoT 서비스와 상호 연결 운용을 도와주는 서비스
AWS IoT ExpressLink	AWS 파트너가 개발 및 제공하는 다양한 하드웨어 모듈을 지원하는 서비스
AWS IoT Greengrass	AWS IoT를 엣지 디바이스로 확장하여 디바이스가 생성한 데이터에 대해 로컬로 작업하고 클라우드를 관리, 분석 및 장기 저장 용도로 사용할 수 있도록 도와주는 서비스
FreeRTOS	IoT 솔루션에 소형의 저전력 엣지 디바이스를 포함시킬 수 있는 마이크로 컨트롤러용 오픈 소스 실시간 운영 체제로서 AWS IoT 서비스를 지원하는 서비스

b. 제어 서비스 영역

제어 서비스 영역은 AWS IoT Core 를 통해 연결된 디바이스가 Cloud 애플리케이션 및 다른 디바이스와 안전하게 상호 작용할 수 있도록 도움을 주며 유효성 검사, 보안 관리 등 디바이스를 관리해 주는 영역으로 상세 서비스는 다음과 같다.

infosec

서비스 명	설명
AWS IoT Core	연결된 디바이스가 클라우드 애플리케이션 및 다른 디바이스와 안전하게 상호 작용할 수 있게 해주는 관리형 클라우드 서비스
AWS IoT Core Device Advisor	디바이스 소프트웨어 개발 중에 IoT 디바이스의 유효성을 검사하기 위한 클라우드 기반의 완전 관리형 테스트 서비스
AWS IoT Device Defender	IoT 디바이스를 보호하는 데 도움을 주며 AWS IoT Device Defender는 IoT 구성을 지속적으로 감사하여 AWS에서 정의한 보안 모범 사례에서 벗어나지 않도록 돕는 서비스
AWS IoT 디바이스 관리	연결된 디바이스를 추적, 모니터링 및 관리하며 디바이스 액세스, 디바이스 상태 모니터링, 문제 감지 및 원격 문제 해결을 위한 보안 터널링과, 디바이스 소프트웨어 및 펌웨어 업데이트를 관리해 주는 서비스

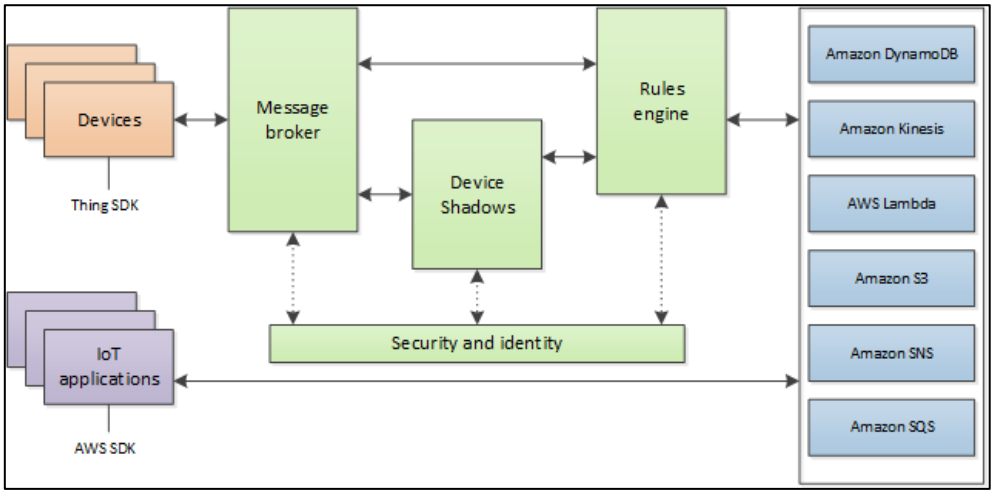
c. 데이터 서비스 영역

데이터 서비스 영역의 경우 AWS 내에서 제공하는 다양한 IoT 서비스들을 활용하여 사용자의 디바이스 내 데이터를 분석 및 모니터링을 제공하는 영역으로 상세 서비스는 다음과 같다.

infosec

서비스 명	설명
Amazon Kinesis Video Streams	디바이스에서 AWS 클라우드로 라이브 비디오를 스트리밍할 수 있게 하며 내구성 있게 저장, 암호화 및 인덱싱 되어 사용하기 쉬운 API를 통해 데이터에 액세스할 수 있도록 도와주는 서비스
AWS IoT Analytics	대량의 IoT 데이터에 대해 정교한 분석을 효율적으로 실행하고 자동화해 운영할 수 있도록 도와주는 서비스
AWS IoT 이벤트	IoT 센서 및 애플리케이션의 이벤트를 감지하며 데이터를 지속적으로 모니터링하고 AWS IoT Core, IoT SiteWise, DynamoDB 등의 다른 서비스와 통합하여 사용할 수 있는 서비스
AWS IoT FleetWise	차량 데이터를 실시간으로 수집하여 클라우드로 전송하는 데 사용할 수 있는 관리형 서비스
AWS IoT SiteWise	게이트웨이에서 실행되는 소프트웨어를 제공하여 MQTT 메시지 또는 API에 의해 산업 장비에서 전달된 데이터를 대규모로 수집, 저장, 구성 및 모니터링을 해주는 서비스
AWS IoT TwinMaker	다양한 실제 센서, 카메라 및 엔터프라이즈 애플리케이션의 측정 및 분석을 사용해 디지털 시각화를 생성하여 실제 공장, 건물 또는 산업 공장을 추적하는 데 도움을 주는 서비스

앞서 설명한 AWS IoT 아키텍처를 이용하여 설계한 모델은 다음과 같다.



[AWS IoT 통신/연결 아키텍처]

2) Azure (Microsoft Azure)

Azure IoT 는 IoT 자산을 연결, 모니터링 및 제어하는 Microsoft Cloud 의 관리형 플랫폼 서비스다. IoT 애플리케이션의 개발, 데이터 분석, 운영 관리 등의 다양한 Native 서비스를 제공하며 Azure 내 다른 서비스와 통합하여 사용할 수 있게 해준다. Azure 의 경우 IoT 서비스를 크게 2 개 영역(연결 및 분석, 에지 및 디바이스 지원)과 8 개 서비스로 구분해 제공하고 있다.

각 영역 및 세부 서비스에 대해 자세히 살펴보면 다음과 같다.

a. 연결 및 분석 영역

연결 및 분석 영역은 IoT 디바이스와 Azure Cloud 서비스 간에 중앙 허브 역할을 하며 안정적인 통신을 가능하게 해주고, 대용량의 데이터를 분석 및 관리를 하는 영역이다.

infosec

서비스 명	설명
Azure IoT Hub	양방향 통신 기술을 지원하면서 디바이스의 원격 상태 파악, 업데이트 및 분석 등의 기능을 제공. 또한 디바이스 프로비저닝을 자동화해 IoT 게시, 배포관리를 도와주며 모든 디바이스를 인증해 보안을 강화하도록 도와주는 서비스
Azure IoT Central	IoT 솔루션 만들기를 간소화하는 IoT 애플리케이션 플랫폼(aPaaS)으로서 대규모 디바이스를 연결, 관리 및 작동하도록 UX 및 API를 제공해 주는 서비스
Azure Digital Twins	디지털 모델을 기반으로 트윈 그래프를 생성할 수 있는 PaaS(Platform as a Service) 서비스로서 디지털 모델을 사용하여 더 나은 제품, 최적화된 작업, 비용 절감 등의 정보를 얻을 수 있도록 도와주는 서비스

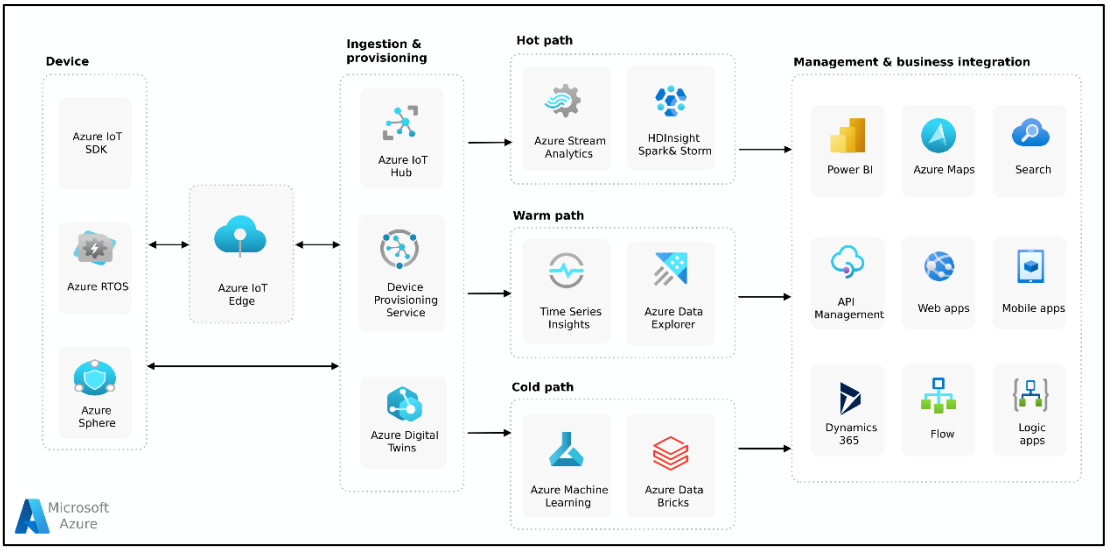
b. 에지 및 디바이스 지원 영역

에지 및 디바이스 지원 영역은 Azure 를 통해 IoT 디바이스 개발 시 이벤트 프로세싱, 머신러닝, 이미지 처리와 같은 복잡한 기술을 손쉽게 배포 및 도입할 수 있게 하는 영역이다. 또한, 인터넷과 연결된 디바이스를 위한 통신 및 보안 기능을 제공해 기기를 제어하며 애플리케이션에 대한 사용자 및 디바이스 액세스를 관리해 준다.

infosec

서비스 명	설명
Azure IoT Edge	Azure IoT Edge 서비스는 세 가지 구성 요소로 이루어져 있다. ① IoT Edge 모듈 : Azure 서비스, 타사 서비스 또는 사용자 지정 코드를 실행하는 컨테이너로, IoT Edge 지원 디바이스에 배포되어 해당 디바이스에서 로컬로 실행 ② IoT Edge 런타임 : 각 IoT Edge 지원 디바이스에서 실행되어 각 디바이스에 배포된 모듈을 관리 ③ 클라우드 기반 인터페이스 : IoT Edge 지원 디바이스를 원격으로 모니터링 및 관리
Azure Percept	Edge에서 IoT 및 AI를 사용하여 비즈니스 전환을 가속화하기 위해 설계된 하드웨어, 소프트웨어 및 서비스 제품. 하드웨어에서 서비스까지 전체 스택을 포괄하여 Edge AI의 통합 문제 해결에 도움을 주는 서비스
Azure Sphere	인터넷에 연결된 디바이스에 대한 기본 제공 통신 및 보안 기능을 갖춘 보안이 강화된 고급 애플리케이션 플랫폼
IoT용 Windows	엔터프라이즈급 기능, 보안 및 관리 효율성을 사물 인터넷에 제공하는 Windows 제품군으로 Windows에 포함된 환경, 에코시스템 및 클라우드 연결을 활용하여 조직에서 신속하게 프로비저닝 되고, 쉽게 관리되며 전체 클라우드 전략에 원활하게 연결할 수 있는 보안 디바이스를 사용하여 해당 사물 인터넷을 만들 수 있도록 지원을 해주는 서비스
Azure RTOS	IoT(사물 인터넷) 및 MCU(마이크로 컨트롤러 장치)로 구동되는 에지 장치용 RTOS(실시간 운영 체제)

앞서 설명한 서비스들로 구축한 Azure IoT 아키텍처는 다음과 같습니다.



[Azure IoT 아키텍처]

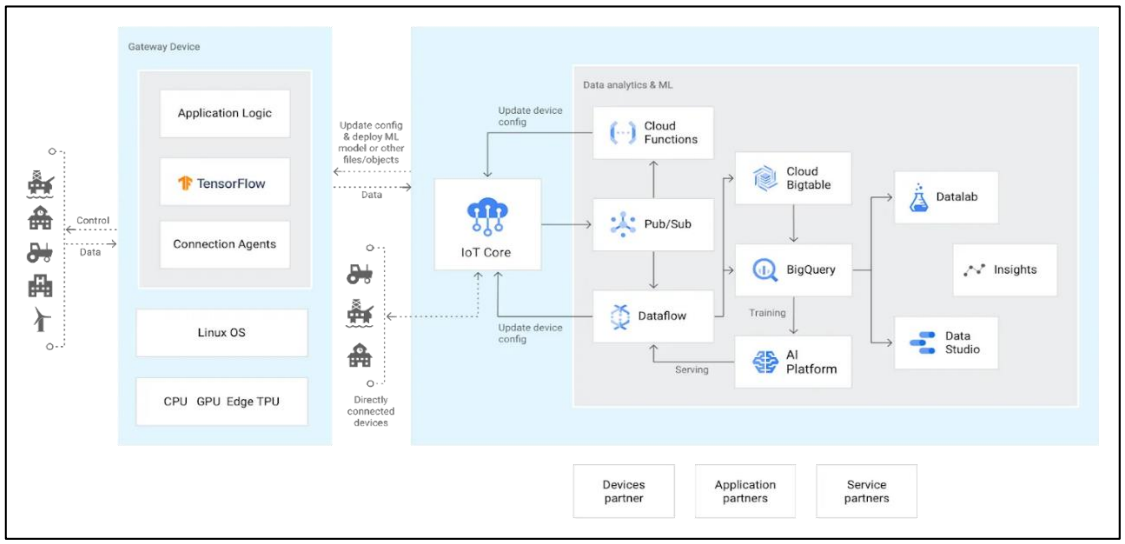
3) GCP (Google Cloud Platform)

Google Cloud IoT Core 는 다양하게 분산된 기기에서의 데이터를 간편하고 안전하게 연결, 관리, 수집하는 완전 관리형 서비스로서 연결된 기기에서 데이터를 수집하고 Google Cloud 의 다른 서비스와 통합되어 사용이 가능하다.

GCP 의 경우 IoT 서비스를 단일 영역 1 개 Core 서비스와 그 외의 관련 서비스로 구분해 제공하고 있다. GCP Native 서비스인 Pub/Sub 를 기반으로 분산된 디바이스의 데이터를 Google Cloud 내 Native 서비스와 통합하여 사용하며 고급 분석, 시각화, 머신러닝 등에 자체 IoT 데이터 스트림을 활용하여 운영 효율성을 높이고 기술·최적화하는 효율적인 모델을 구축할 수 있게 해준다.

※ 2023 년 8 월 16 일부터 Google Cloud 의 IoT Core 서비스는 종료가 될 예정이며 대체 서비스로 AWS 의 'IoT 코어'나 Azure 의 'IoT 허브'가 거론이 되고 있는 상태이며 Google Cloud IoT 도입할 경우 타 CSP 의 IoT 서비스를 고려해야 한다.

(https://cloud.google.com/iot/docs)



[Google Cloud Platform IoT 아키텍처]

1. 보안 고려 사항

지금까지 CSP(AWS, Azure, GCP)에서 제공하는 IoT 서비스에 대해 간략히 살펴봤다. 다음으로 CSP 에서 제공하는 IoT 서비스를 Cloud 환경 안에서 기기들과 연결해 사용할 때 고려해야 하는 보안 사항들에 대해 알아보고자 한다.

기본적으로 3 곳의 CSP 모두 고객 및 비즈니스의 데이터 보호를 위해 자체적인 보안 규정을 준수하고, 표준 보안 프로토콜 및 안전성이 검증된 암호 알고리즘을 지원하며, 연결된 기기와 Cloud 간에 안전한 양방향 통신을 제공한다. 또한, 사용자 및 기기에 대한 자체 자격 증명 및 액세스 관리를 지원해 고객으로 하여금 안전하게 권한을 부여해 사용할 수 있도록 자체적인 Native 서비스(AWS IAM, Azure RBAC, Azure AD, GCP IAM 등)를 제공하고 있다. 마지막으로, 가상 네트워크 환경을 통해 공용 인터넷에 대한 연결 노출을 제한해 IoT Core/Hub 등을 사용할 수 있으며, 그 외에 서비스 운용의 안전성 및 가용성 등의 보안이 고려될 수 있도록 다양한 Native 서비스들을 IoT 서비스들과 함께 사용할 수 있도록 지원한다.

1) 인증 및 자격 증명 관리

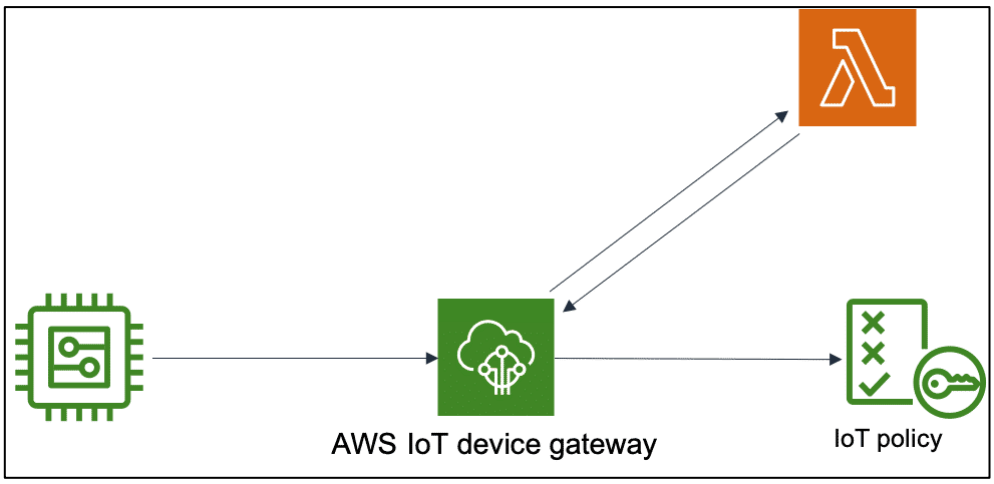
연결된 디바이스 및 사용자에 대해 사용 용도 및 역할에 맞는 액세스 제어를 해야 하며 'principle of least privilege(최소한의 원칙)'가 적용될 수 있게 구체적이고 세부적인 권한에 대한 자격 증명을 마련해야 한다. 또, 액세스를 안전하게 관리할 수 있는 정책을 내부적으로 만들어 관리해야 한다.

IoT Cloud 에서의 인증은 서버 또는 클라이언트의 자격 증명을 확인하는 것이다. 서버 인증은 디바이스 또는 다른 클라이언트가 Cloud 의 IoT 엔드포인트와 통신하는 것이며, 클라이언트 인증은 디바이스 또는 다른 클라이언트가 CSP 의 IoT 서비스를 사용하여 인증하는 프로세스다. 이를 통해 IoT 기기와 연결된 모든 장치는 승인되지 않은 클라이언트 및 서버의 입력이나 요청을 수락하지 않도록 해야 한다.

인증의 경우 CSP 마다 인증 방식이 조금 상이할 수 있으며, 사용 중인 장치의 유형이나 아키텍처 및 인프라에 따라 다르게 적용된다. 기기/애플리케이션/CLI 명령 등 IoT 서비스 연결 및 이용 시 각 CSP 에서 제공하는 인증 방법들과 대표적으로 사용되는 한 가지 방법에 대해 알아보자.

a. AWS

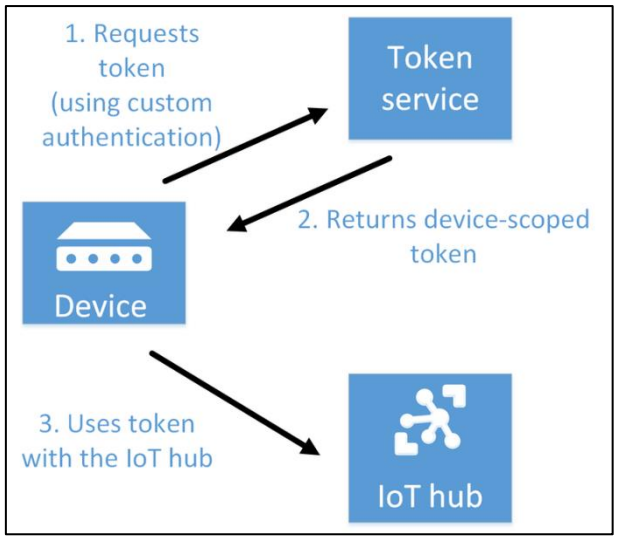
AWS 의 경우 X.509 certificate, 사용자 지정 인증, Amazon Cognito, IAM, 자격 증명 등의 인증을 사용한다. 여러 인증 방식 중 사용자 지정 인증의 경우 사용자 지정 권한 부여자와 함께 사용자 지정 인증 서비스와 AWS Lambda 함수를 사용하여 자체 인증 및 권한 부여 전략을 관리할 수 있다. 사용자 지정 권한 부여자를 사용하여 AWS IoT 는 전달자 토큰 인증 및 권한 부여 JWT 또는 OAuth 를 사용하여 자격 증명을 인증하고 작업을 승인한다.



[AWS IoT 디바이스 게이트웨이 <> 사용자 지정 권한 부여자 인증]

b. Azure

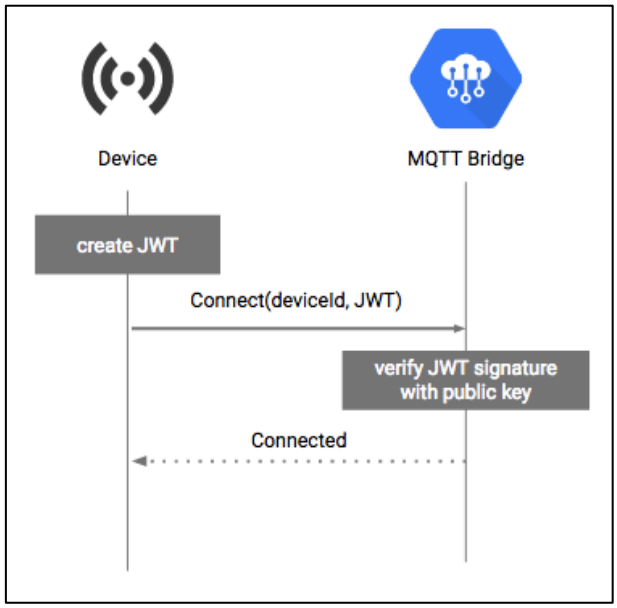
Azure 의 경우 Azure AD, Azure RBAC, X.509 certificate, 등의 인증을 사용한다. Azure 에서 소개하는 RBAC 인증은 IoT Hub ID 레지스트리를 사용하여 토큰을 통해 디바이스/모듈별 보안 자격 증명 및 액세스 제어를 구성할 수 있다.



[토큰 서비스를 통한 디바이스 인증]

c. GCP

GCP 의 경우 IAM, 인증(키/쌍, JWT, 애플리케이션, MQTT 브리지) 등의 방법이 존재한다. 아래 그림은 MQTT 를 사용해 Cloud IoT Core 에 인증하는 과정을 요약한 그림으로 MQTT 브리지는 기기의 공개 키와 대조해 JWT 를 확인해 연결한다.



[MQTT 브리지 사용을 통한 Cloud IoT 인증]

마지막으로, 인증 키는 배포 시에 Cloud 서비스에서 생성된 장치 ID 및 관련 인증 키가 필요하기 때문에 키 저장, 키 순환 등의 보안 요소를 고려해 키를 안전하게 관리하고 각 장치에는 고유한 암호를 생성해 관리해야 한다.

2) 연결 보안

AWS, Azure, GCP 모두 TLS(전송 계층 보안)를 지원하며, 이를 통해 IoT 디바이스 및 서비스의 연결을 보호한다. 또한, CSP 에서 제공되는 가상 네트워크 환경에서의 엔드포인트 및 Native 서비스(AWS PrivateLink, Azure Private Link)를 지원해 프라이빗 IP 주소를 통해 CSP 에서 실행되는 서비스에 대해 안전하게 액세스하여 외부에서의 노출을 최소화시켜 서비스를 이용할 수 있다.

3) 데이터 보안

디바이스와 클라우드 환경 및 클라우드 서비스 간의 저장, 전송 중인 데이터들에 대한 암호화를 해야 하며 암호화는 보안상 안전한 프로토콜(MQTT, HTTPS) 및 알고리즘을 사용해 데이터를 보호해야 한다. 대부분의 CSP 들은 기본적으로 전송에 대한 데이터 보호를 지원하고 있으며 저장 시의 데이터 암호에 대해서는 별도 설정 및 옵션의 형태로 데이터를 보호해 준다. 데이터 암호 시에는 자체 CSP 소유의 키를 사용해 암호화할 수도 있다.

4) 로깅 모니터링 및 보안 솔루션

CSP 에서 제공되는 모니터링 및 로깅 Cloud Native 서비스(Cloud Watch, Cloud Trail, Azure Monitor, Cloud Logging …) 등을 활용해 비정상 행위 및 접근 등의 보안 위협에 대비해야 하며, CSP 별 보안 솔루션(AWS: Security Hub, Azure: Security Center, Google: Security Command Center)에서 제공하는 다양한 보안 도구 및 기능을 활용해 보안을 강화할 수 있다. 그 외에도 일부 CSP 는 IoT 서비스를 더욱더 안전하게 사용하기 위한 맞춤 보안 서비스들을 제공한다. AWS 의 경우 기기들의 구성 감사 및 모니터링 등을 수행해 보안 위험을 완화할 수 있도록 도와주는 “IoT Device Defender” 서비스를 제공하며, Azure 는 IoT 및 OT 디바이스, 취약성 및 위협을 식별하는 통합 보안 솔루션인 “Microsoft Defender for IoT”를 제공해 보안성을 향상시킬 수 있는 방법을 제안하고 있다.

마치며, 위에서 설명한 4 가지의 Cloud 환경에서 IoT 보안 고려사항 외에도 IoT 에 대한 기본적인 보안(펌웨어 보안, 하드웨어 취약점, WebCM 애플리케이션 취약점, 불필요 서비스 사용 등)에 대해서도 신경을 써야 한다. CSP 에서 제공하는 보안에 특화된 Native 서비스 또는 솔루션만 사용하지 말고 컴퓨팅, 네트워크, 애플리케이션 등의 모든 계층에서의 보안성 향상을 위해 다른 Cloud Native 서비스 및 리소스를 함께 사용함으로써 외부 위협으로부터 디바이스 및 Cloud 환경을 안전하게 구성해야 한다.

참고자료

공통

https://www.n-ix.com/best-practices-ensure-iot-cloud-security/

https://www.techtarget.com/iotagenda/

https://www.iotforall.com/iot-cloud-convergence-security-guide

https://www.cloudflare.com/ko-kr/learning/security/glossary/iot-security/

AWS

https://pages.awscloud.com/rs/112-TZM-766/images/IoT_Security_Best_Practices_Guide_design_v3.1.pdf

https://docs.aws.amazon.com/ko_kr/iot/

https://aws.amazon.com/ko/iot-core/faqs/

Azure

https://docs.microsoft.com/ko-kr/azure/iot-fundamentals

https://docs.microsoft.com/ko-kr/azure/iot-edge/about-iot-edge?view=iotedge-2020-11

https://docs.microsoft.com/ko-kr/azure/architecture/reference-architectures/iot

https://docs.microsoft.com/ko-kr/azure/iot-hub

https://docs.microsoft.com/ko-kr/azure/defender-for-iot/

https://docs.microsoft.com/en-us/security/benchmark/azure/baselines/iot-hub-security-baseline

https://docs.microsoft.com/en-us/azure/role-based-access-control/

Google Cloud

https://cloud.google.com/iot-core

https://cloud.google.com/iot/docs/concepts/device-security

https://www.kcloudnews.co.kr