Analyse comparative des solutions IoT

Azure IoT Hub
vs
EdgeX Foundry

Realisé par :

FEKI Emna

Introduction

L’Internet des Objets évolue rapidement et impose de choisir des plateformes capables de gérer efficacement la diversité des appareils connectés. Deux approches dominent aujourd’hui : les solutions cloud comme Azure IoT Hub et les architectures edge computing telles qu’EdgeX Foundry. Ce choix influence directement la performance, les coûts et la sécurité des projets IoT.

Ce travail propose une comparaison concise entre ces deux plateformes, en analysant leurs architectures, leurs fonctionnalités clés et leur comportement dans un petit scénario simulé reliant un capteur virtuel à un tableau de bord. La démarche combine une courte revue bibliographique et une simulation simple d’un flux IoT.

Cette étude offre une vision synthétique des forces et limites de chaque solution et permet de mieux situer leur pertinence dans le contexte IoT actuel.

Présentation des plateformes

Microsoft Azure IoT Hub : Une solution Cloud-Native

Azure IoT Hub est une plateforme cloud de Microsoft permettant de connecter, superviser et contrôler un grand nombre d'appareils IoT. Elle offre des fonctionnalités clés comme la sécurité avancée (TLS, certificats), les mises à jour OTA et l'intégration avec les services AI/ML d'Azure. Sa scalabilité et sa robustesse en font une solution adaptée aux déploiements à grande échelle.

EdgeX Foundry : L'intelligence au plus proche des Données

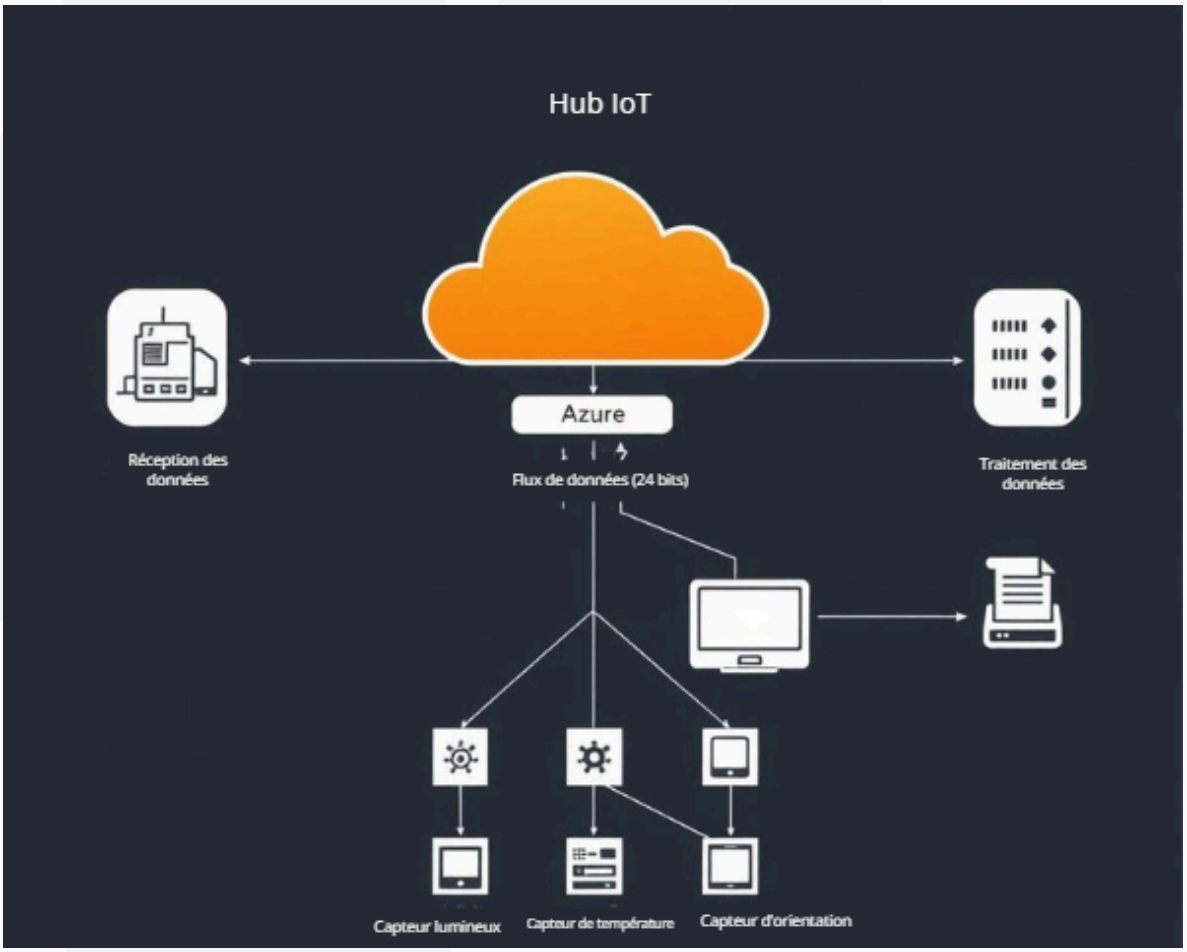
EdgeX Foundry est une plateforme open-source orientée edge computing, conçue pour traiter les données directement au niveau local. Elle se distingue par sa modularité, sa capacité à réduire la latence et à préserver la confidentialité des données, tout en offrant des services flexibles pour l'intégration avec divers capteurs et protocoles.

Présentation des plateformes

Architecture générale

<u>Microsoft Azure IoT Hub :</u> Une solution Cloud-Native:

Azure IoT Hub adopte une architecture cloud centrée sur un hub central chargé de gérer la communication sécurisée entre les appareils et les services Azure. Les données issues des capteurs sont transmises vers le cloud, où elles peuvent être stockées, analysées ou intégrées à des services avancés comme Digital Twins et IoT Edge.

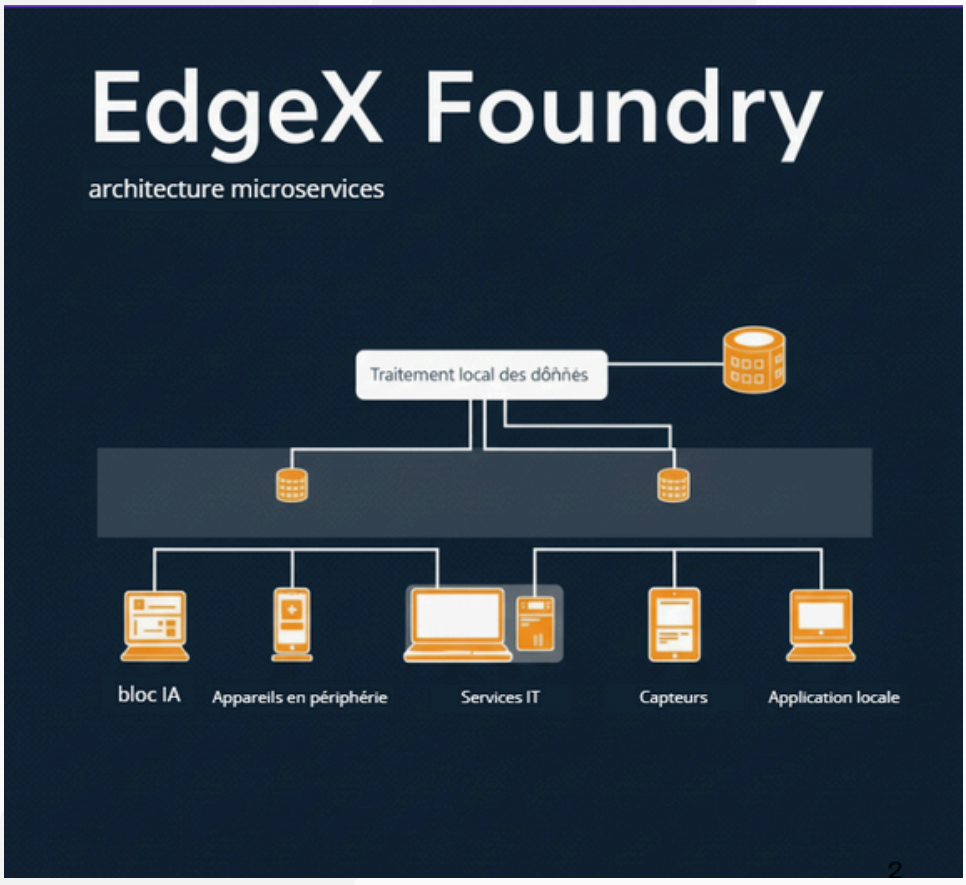


Présentation des plateformes

Architecture générale

EdgeX Foundry : L'intelligence au plus proche des Données

EdgeX Foundry repose sur une architecture de microservices déployés à la périphérie, permettant de collecter, traiter et filtrer les données directement au niveau local. Les device services captent les données des capteurs, les core services les organisent, puis les application services les exportent vers d'autres systèmes ou plateformes.



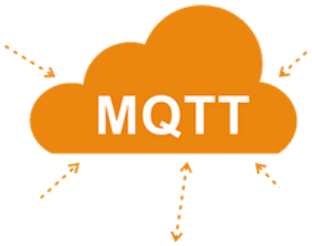
Onboarding et outils

Azure IoT Hub : Simplicité et Intégration

- Inscription rapide via le portail Azure et création d'un IoT Hub.
- configure sa communication via MQTT ou HTTPS à l'aide des clés d'authentification
- Enregistrement des appareils facilité par le Device Provisioning Service (DPS).
- SDKs multilingues (C, Java, Python, .NET) pour un développement agile.
- Outils intégrés comme Azure CLI, Azure Portal, et Azure IoT Explorer pour une gestion et un monitoring efficaces.
- Support du déploiement continu et des mises à jour OTA via Azure IoT Edge.

EdgeX Foundry : Flexibilité et Communauté

- Installation sur les périphériques edge via conteneurs Docker ou déploiement natif.
- Configuration modulaire des microservices, adaptée aux besoins spécifiques.
- Utilisation d'API REST et MQTT pour une intégration transparente des appareils.
- Outils open-source, notamment les Device Services pour la découverte et la gestion des capteurs/actionneurs.
- Une communauté active et une documentation riche pour une personnalisation avancée.



Sécurité : authentification, certificats, rôles, gestion TLS

Sécurité Robuste avec Azure IoT Hub

- **Authentification :** Certificats X.509, clés symétriques ou TPM.
- **Gestion des rôles :** Contrôle d'accès basé sur les rôles (RBAC) via Azure Active Directory.
- **Communication :** TLS 1.2 obligatoire pour toutes les communications.
- Surveillance : Surveillance continue avec Azure Security Center IoT.
- **Automatisation :** Support de la rotation automatique des clés et certificats.

Sécurité Modulaire avec EdgeX Foundry

- **Authentification :** Basée sur certificats X.509 et tokens JWT.
- **Sécurité des services :** Support TLS pour la communication inter-services;
- **Gstion des accés :** Mécanismes intégrés ou extensions personnalisées.
- **Personnalisation :** Hautement configurable pour répondre à des besoins spécifiques.
- **Dépendance :** La robustesse dépend fortement de la configuration locale et des bonnes pratiques de déploiement.

Analyse coûts, modèle économique et limites

Azure IoT Hub : Modèle SaaS évolutif

Les coûts augmentent selon le volume de messages, les unités IoT et les services Azure utilisés.

Basé sur un système pay-as-you-go entièrement dépendant du cloud Microsoft.

Dépendance totale au cloud, coûts élevés pour les déploiements massifs et latence liée au réseau.

EdgeX Foundry : Open-Source et Maîtrise Locale

Gratuit et open-source, seuls les coûts d'infrastructure locale et de maintenance sont à prévoir.

Aucune licence, modèle communautaire open-source reposant sur un déploiement edge autonome.

Déploiement plus complexe, absence d'outils analytiques natifs et besoin de ressources edge adaptées.

Étude comparative et applications IoT

	Azure IoT Hub : Modèle SaaS évolutif	EdgeX Foundry : Open-Source et Maîtrise Locale
Architecture	Cloud centralisé	Edge modulaire en microservices
Sécurité	TLS, IAM, certificats	TLS, certificats
Coût	Payant (scalable à l'usage)	Gratuit (open-source)
Avantages	Haute scalabilité, intégration AI/ML, gestion cloud simplifiée	Traitement local rapide, confidentialité, modulairité
Limites	Coût élevé à grande échelle, dépendance au cloud	Déploiement complexe, peu d'analytique natif
Protocoles	MQTT, AMQP, HTTP	MQTT, Modbus, BACnet, HTTP
Cas d'usage	les smart cities, la maintenance prédictive et les véhicules connectés	l'industrie 4.0, la santé ou la surveillance en temps réel

Merci pour votre attention

@FEKI Emna