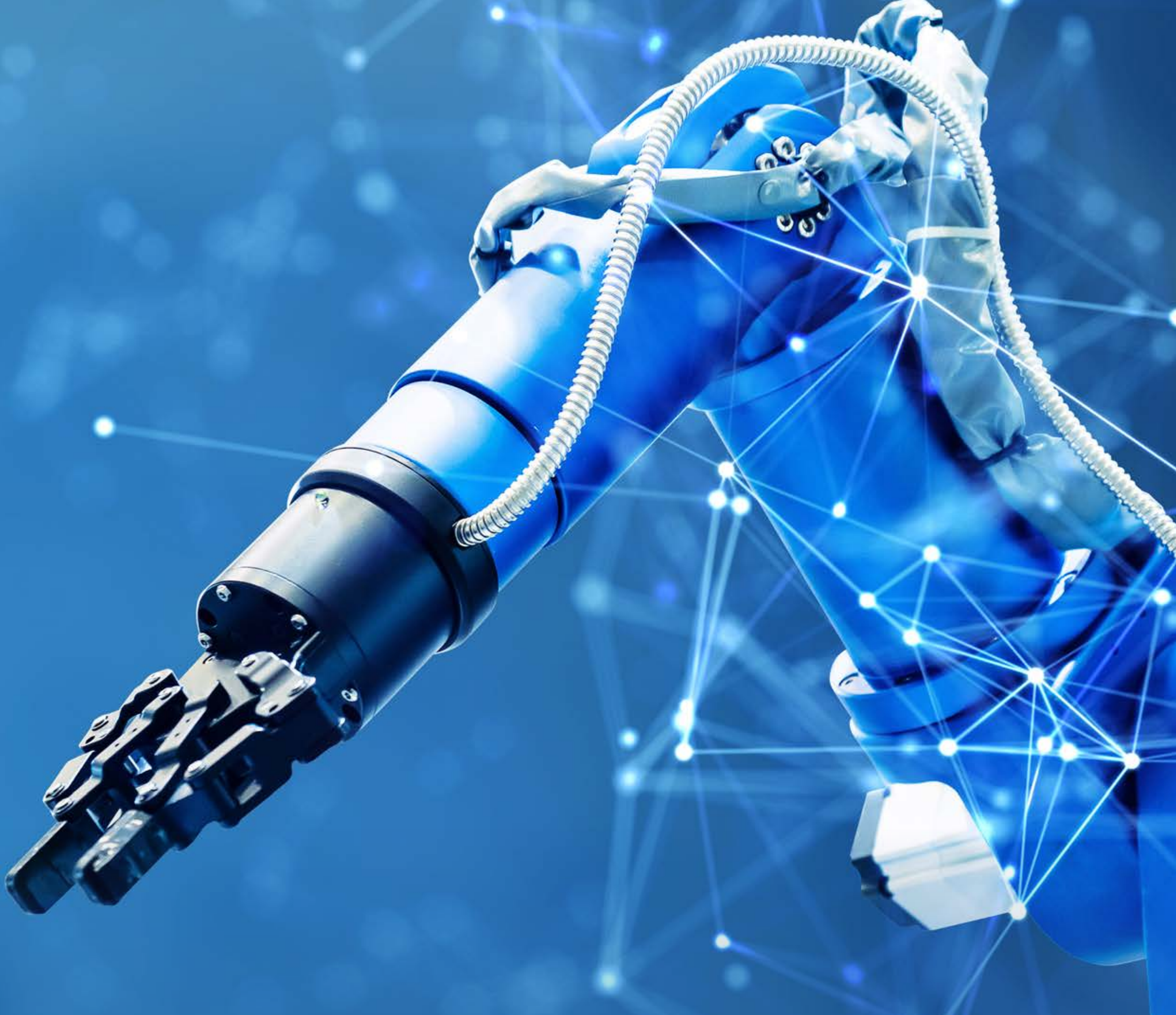

ANALYST REPORT

How intelligence at the edge powers endless optimisation for IoT use cases

Report sponsor:

eseye

Intelligence at the edge powers endless optimisation for IoT use cases

In the first half of 2024, the pendulum has swung away from cloud obsession to increased reliance on edge intelligence that allows IoT organisations to gather the insights and information that use cases need to operate effectively. That doesn't mean it's time to dump your Amazon, Google or Microsoft stock but it does mean that IoT organisations are more carefully assessing when to utilise cloud. They are looking closely and adopting alternatives to centralised cloud, taking advantage of improved economies of scale, advances in processing capability and the ability to apply artificial intelligence and other processing within their IoT devices ▶

SPONSORED REPORT

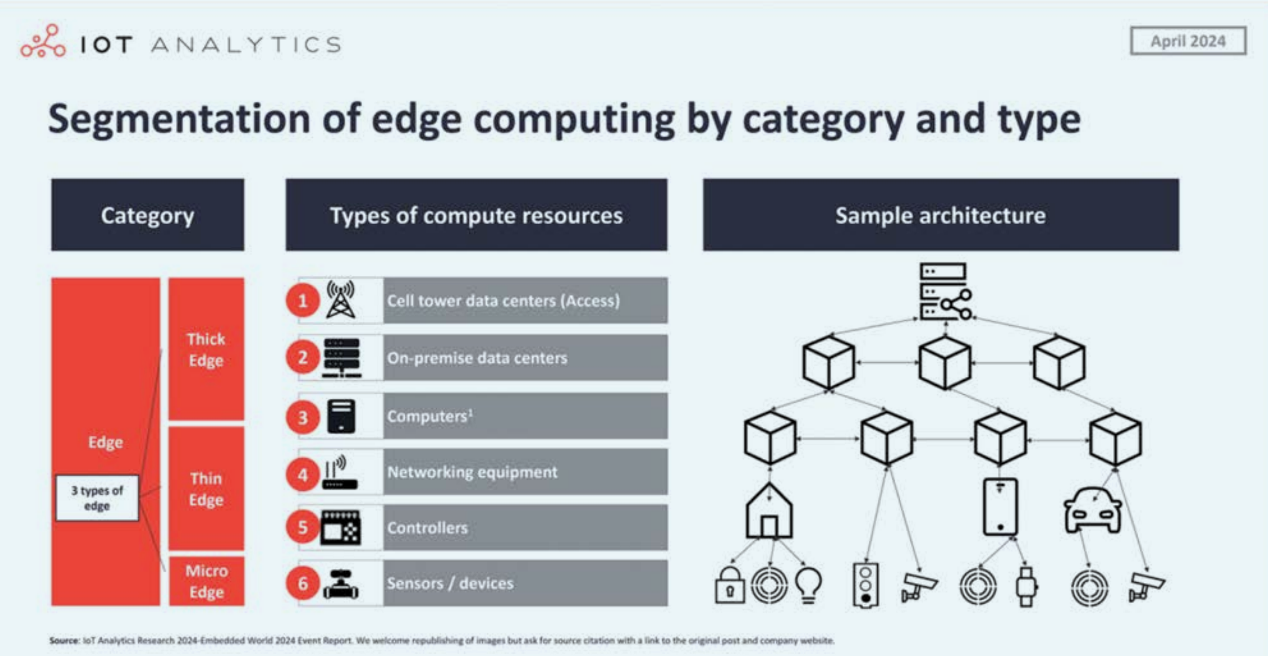

Figure 1: Intelligence has many edges
Source: IoT Analytics, 2024

The right answer isn't always to roll-out massive volumes of dumb devices at the lowest unit cost possible, relying on resilient wireless connectivity and vast public cloud resources to deliver the desired outcome. Instead, today, with increasing regularity, the correct decision is to use the increased processing at the edge and add intelligence either in the devices themselves or in nearby hardware such as smart home hubs or resources at the network edge that can aggregate information and process it to derive valuable insights and outcomes. Not everything has to go to a centralised cloud computing resource for analysis to determine what action to take and then be communicated back to the device. Increasingly decisions can be made on the device or closer to it, reducing latency of roundtrip transmissions.

Edge intelligence reduces network and cloud payloads

Increased analytics outside of cloud data centres is in line with Gartner analyst, Santhosh Rao's 2016 prediction that 'by 2025, 75% of enterprise-generated data will be created outside the traditional data centre or cloud.' It's now clearer that the 'outside' of Rao's vision is composed of intelligent edge devices and vast volumes of data will be created – and acted upon – by these devices.

Had the established practice of sending everything to the cloud continued uninterrupted, IoT development would have been slowed because the network would not be able to keep up with the vast amount of data needing to be communicated in the massive IoT era. On top of this, organisations would face crippling cloud computing costs in the form of network charges as well as unacceptable latency for some use cases. In addition, don't forget that, while cloud itself has offered greater flexibility than monolithic IT infrastructure, it has never been free and power and cooling costs continue to rise.

Devices need to be network aware

The trend away from cloud puts pressure back on IoT device designers who need to add processing capabilities into their devices to power edge intelligence. These devices still need the capability to communicate autonomously, often with both low power, local communications technology and long range, high-bandwidth cellular technology. Alongside that they need processing power and the ability to perform functions via actuators, sensors and application-specific systems.

IoT now starts and ends with the device so designers and developers are looking to boost device functionality with ▶

The trend away from cloud puts pressure back on IoT device designers who need to add processing capabilities into their devices to power edge intelligence

smart modules, multiple connectivity – or radio access technology (RAT) – capabilities, the early application of AI and machine learning and utilisation of more granular sensors that can collect and analyse inputs across multiple data points. These are all essential to create, augment, support and contribute to the overall performance of an IoT offering. A key aspect of this is ensuring that distributed data are able to move around the network as required.

The challenge facing IoT organisations as they adopt intelligence at the edge is also an opportunity. If you think of a connected water sensor, it's counter-productive for data to be sent to the cloud for processing which results in action being taken to sound an alarm. Instead, a more intelligent device can sound an immediate alarm to warn residents of a leak and therefore the sensor needs to have the capability to take the sensor data and trigger an alarm all on one device with minimised latency and cost.

More complex, less urgent tasks optimised

This isn't where the value of the product ends, though. There are other analyses the sensor can perform and non-urgent data that it collects, such as information on monthly consumption or temperature data, can contribute to the overall service value. The optimal blend is to utilise device intelligence at the edge to deal with straightforward, mission critical, time-specific requirements alongside connection to the cloud for processing of additional, potentially more complex but less urgent data that can be combined with other data sets. Depending on the use case, these data may be more complex and require greater compute power or involve processing of larger data sets to derive insights and value.

There's a clear divergence of computing needs between the local, time-sensitive use cases that have a limited processing burden and the distributed, non-urgent value propositions that require in-depth analysis and, potentially, inputs from multiple devices. On-device, edge intelligence, powered by advances such as machine learning, enables that very fast, lighter weight processing to be completed at a cost that is increasingly acceptable to IoT business cases. On the other hand, cloud computing enabled by robust, secure, compliant and trusted connectivity, delivers the foundation for analysing terabits of data from hundreds of thousands of devices and sensors. In most instances, edge and cloud computing can be combined to address deliver different parts of a solution. For example, the water sensor would notify the person in the house with an audible alarm while the cloud would be used to send a text message and provide more

comprehensive analytics on increasing humidity levels that may be an early indicator.

There is, of course, a middle ground in which intelligent edge devices operate to gather and explore data from a network of local devices. Not all of these data go all the way to the cloud, some is processed on these devices, allowing for very cost-effective connected sensors that communicate to the local device, potentially using ▶

Cloud data must be accessible to devices, device data must be accessible to edge computing resources, edge resources must be able to access cloud data and the IoT devices themselves

efficient low power wide area (LPWA) connectivity. As network technologies proliferate, with the addition of non-terrestrial networks (NTNs) to the mix, IoT services can take advantage of different networks in different situations. In a fleet tracking scenario, for example, the vehicle may use an NTN when it is out of cellular coverage, cellular coverage while in a city and Wi-Fi when back at base to upload routine data. IoT is becoming increasingly network-aware with devices and data needing to behave differently according to the network resources available at any given time.

Balance performance, latency, availability and cost

To help enable this intelligent switching between networks to use the most appropriate for a given task, **Eseye** has developed its SMARTconnect offering which includes a range of APIs designed to optimise edge intelligence with connectivity. The network aware API, in particular, provides an IoT application with information on the network state to help it prioritise and transmit data, switching between networks based on availability and signal strength, data volume and frequency, power consumption, compliance and security. While the SMARTconnect system can calculate some of these answers itself, it also needs to be told about information such as the network cost in order to make an optimised decision.

A system that isn't able to assess the full picture, can't hope to succeed. For example, a system could decide that utilising 5G is the best way to upload some video data from an application may break the business case because the – unknown – cost of 5G in that location is more than the fee charged for the service can support.

SMARTconnect has the intelligence to balance out a wide range of factors to arrive at the best network for the use case at that time in that location. It's the opposite of a one-size-fits all approach to IoT connectivity, fitting the best available network to the use case and switching when better options become available. This is simplified because SMARTconnect can work autonomously with no need for real-time instructions from an IoT network. ▶

Right size, not one-size

Effectively right-sizing connectivity for the job at hand and having the flexibility to switch to an alternative when the job or situation changes is integral to enabling edge intelligence. The knowledge that fuels smart connectivity is also applicable to supporting more business, life and mission critical applications across IoT. The same intelligence applied to connectivity can be repurposed to support end-to-end security, compliance and trust and this means complex applications, such as those in healthcare, can be enhanced (**see Case Study p33**).

By knowing how the device is reacting and seeking to ensure relevant data has transmitted to the edge devices or cloud resources that it needs to access, applications can be assured that the network is operating as expected, that the network hasn't been compromised and that regulations for financial services or data sovereignty have not been broken. One example use case is carbon trading. The high value of the sector means that a significant amount of fraud occurs and device authentication, authorisation and encryption are prerequisites.

It is very important for carbon trading participants to have an audit trail that demonstrates end-to-end support for ISO14064-2 and smart software is needed to provide complete auditability for linking devices together. Carbon trading is one of the better known use cases for blockchain and it relies on end-to-end security. In this example, SMARTconnect would have the secure credentials because it not only ensures secure connectivity is provided but also because it has insight into device CPU utilisation, supports IoT SAFE and combines intelligence on the device with local interconnected and breakout traffic to ensure the route taken from the device to the cloud is compliant.

Expanded intelligence at the edge

Recent innovation in the forms of AI, the return to more-than-Moore's Law processor advances and greater network technology choice have transformed the practicality of edge intelligence. This has happened at a time when cloud costs, environmental impacts and security are under heightened scrutiny. It's therefore no surprise that, with IoT set to cement itself as a hyperscale sector, participants are looking to optimise their operations.

Edge intelligence starts with cleverly designed IoT devices that balance cost with capability, form factor and power usage. These intelligent devices connect either to the cloud directly or to edge devices where pre-cloud processing can be performed and action taken locally. The connectivity type and network utilised can now be optimised for the data volume and frequency, the financial constraints and the power consumption of the device – and changed almost instantly to reflect the needs of new requirements. That flexibility and continuous ability to optimise across the networks alongside the entire ecosystem is at the heart of IoT's expanded intelligence at the edge.

Download the AnyNet SMARTconnect™ solution paper