EDGESCALE: SOLVING EDGE COMPUTING MANAGEMENT AND SECURITY CHALLENGES

Edge computing stands to transform the IoT much the same way that cloud computing is transforming enterprise IT. By borrowing cloud-computing software technology, edge computing achieves comparable ease of use. By deploying the solution near the point of use and source of data, edge computing enables real-time processing and eliminates an expensive WAN connection to the cloud as a bottleneck to analysis, especially when it comes to large data sets for artificial intelligence and machine learning. However, edge computing presents new challenges to security and device management owing to the proliferation of remote nodes with little to no physical user interface. NXP has developed EdgeScale to address these challenges.

EDGE COMPUTING MANAGEMENT AND SECURITY CHALLENGES

Edge gateways, like other embedded systems, have been appliance-like: fixed in function with hardware and software built for a single application. With the advent of edge computing and the ability to run cloud-based applications away from the data center, these gateways must evolve from appliances to a model where they can be programmed depending on usage and deployment much like a phone, tablet, or PC. In other words, they must evolve from fixed-function communication devices to nodes that also compute at the edge.

The edge-computing nodes implement cloud-computing techniques, hosting serverless functions, containers, and virtual machines, offering applications APIs like those of cloud hosts. Embedded on shop floors, near medical equipment, and in home-automation systems, edge computing nodes support IoT deployments. They provide local computing resources and connect to both nearby IoT endpoints and possibly distant systems.

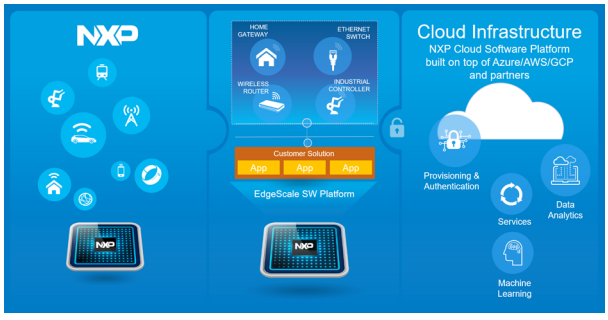
The edge-computing nodes, however, cannot be managed like these devices. They lack the keyboard and display interfaces and may be physically inaccessible after deployment. Moreover, an IT manager may have thousands or even millions of these nodes. Hence, the ability to remotely manage, configure, and update these embedded nodes is both a necessity as well as a challenge.

There are many edge-computing frameworks available today—AWS Greengrass, Azure IoT Edge, Aliyun, Google IoT cloud, and Watson IoT to name a few. They all provide a comprehensive framework for application development, deployment, and communication. However, the process of on-boarding these nodes remains manual and often cumbersome. Most importantly, provisioning of credentials/certificates is not tied down to a hardware root of trust, which leaves these nodes vulnerable to cyberattacks. Hardware root of trust is an approach to computing in which attack-resistant chips process security algorithms as well as key and certificate storage. Hardware-based trust systems are much more robust than software-based systems against cyberattacks.

SOLVING MANAGEMENT AND SECURITY CHALLENGES WITH EDGESCALE

To solve these challenges, NXP developed the EdgeScale suite. The EdgeScale suite automates what is now the manual and cumbersome process of provisioning equipment and updating software. To ensure that this is done securely, the EdgeScale suite leverages NXP's Trust Architecture technology.

This unique implementation of hardware root of trust helps enable essential features like secure boot, secure key storage, manufacturing protection, hardware resource isolation, and runtime tamper detection—key features for providing in-depth security throughout a node's entire lifecycle, including manufacture, software installation, deployment, daily operation, software upgrades, and decommissioning.



EdgeScale simplifies device management by providing device-based tools and software and cloud-based services. These can integrate with any of the popular edge-computing frameworks. Customers have the option of using the EdgeScale suite standalone via the Dashboard or CLI, or using the REST API to integrate with their own management framework.

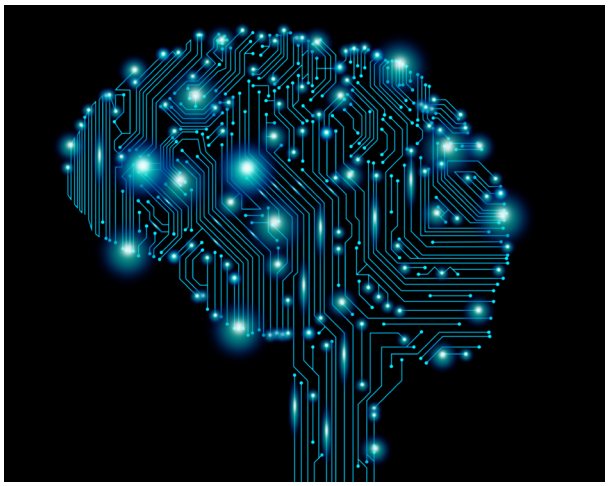
EdgeScale provides customers a choice of which edge-computing framework they want to run, even supporting multiple frameworks simultaneously on the same node. EdgeScale can deploy these frameworks as containers, so switching from one to another can be done on the fly.

EdgeScale can help customers manage their own private cloud with a closed ecosystem of applications being managed internally. In this scenario, EdgeScale services can be hosted locally on premises, with customers having complete control over what is shared externally.

To enable rapid development and deployment from the cloud, EdgeScale also provides a cloud-based SDK. Developers can create applications on the cloud, compile them into containers, and deploy them to multiple edge-computing devices with a click of a mouse.

SUPPORTING ARTIFICIAL INTELLIGENCE THROUGH MACHINE LEARNING

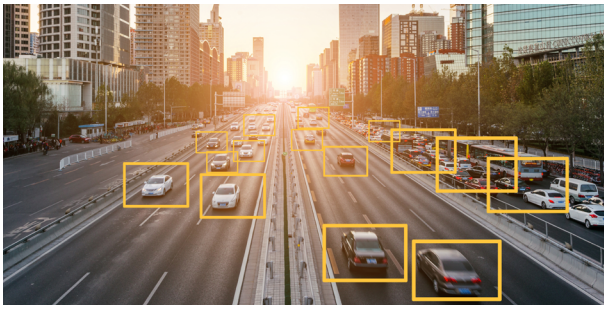
The last several years have seen a rapid increase in the use of machine learning (ML) as a technology to support artificial intelligence (AI) workloads such as Alexa, Amazon's cloud-based voice service. While the Cloud will remain the best place to train ML algorithms, increasingly Edge devices are becoming the best place to execute the inference component of ML and enable AI for whole new classes of systems. ML training is often and rightfully described as GPU-intensive; however, the outcome of cloud-based ML training can be executed very efficiently on multicore Arm® processors.



The power-efficient performance of these Cortex®-A53 and A72-based SoCs assisted by local GPUs or vector processing engines makes NXP's SoC offerings the best choice to run the most popular open-source software libraries for machine learning.

Computer vision algorithms running on edge nodes support the extraction and transmission of semantic data instead of sending raw video streams, thereby reducing bandwidth requirements while enhancing privacy. This allows the broader use of connected video and imaging technology without overwhelming networks.

The EdgeScale suite facilitates the emerging approach of using cloud-based servers or supercomputers for training and edge compute devices for the inferencing stage of ML processing where the AI is utilized. This approach optimizes the accuracy of the algorithm, allows for regular updates while ensuring that the required latency and bandwidth are minimized. This approach also eliminates the need for continuous connectivity to the cloud for system operation and increases the privacy of the subject data, which no longer needs to be transferred to a cloud for processing.



NXP'S ROLE

The scale of an edge-computing node varies depending on its workload. Edge systems range in computing power from low-cost single-core devices up to the equivalent of a data center server. Networking performance ranges from 1Gbps (with 50Mbps loads possible) to 100Gbps. Storage capacity likewise ranges from megabytes of flash to terabytes of hard drive storage. Enabling software, such as the various edge-computing frameworks, makes these capabilities, regardless of scale, appear as generic resources to applications.

To support this range in scale, NXP offers a broad lineup of processors for edge computing from the single-core, sub-1-watt LS1012A to the recently announced 16-core LX2160A. These Layerscape® processors are all equipped with NXP's Trust Architecture and can use EdgeScale to bridge cloud frameworks to edge nodes, sensors, and devices, solving IoT deployment, management, and security challenges.

To support edge-computing frameworks and application development, NXP's Layerscape Software Development Kit includes drivers, tools, and libraries enabling Layerscape processor features. A long-term support release of the Linux® kernel that includes drivers and support for other Layerscape-specific features is available along with an Ubuntu user-land environment. The kernel also supports containers, the lightweight approach favored in cloud computing of bundling the code, libraries, tools, and settings required of a rich application.

To extend these frameworks and make edge-computing nodes easy to target for application development, easy to deploy, and easy to manage, NXP offers EdgeScale. For more information, please contact your local NXP representative or visit www.nxp.com/EDGESCALE.

NXP, the NXP logo, NXP SECURE CONNECTIONS FOR A SMARTER WORLD and Layerscape are trademarks of NXP B.V. All other product or service names are the property of their respective owners. Arm and Cortex are registered trademarks of Arm Limited (or its subsidiaries) in the EU and/or elsewhere. All rights reserved. © 2018 NXP B.V.

Document Number: EDGESCLECATEWPA4 REV 0

Date of Release: March 2018