

Pierre Gembaczka is a lead data scientist at Krohne in Duisburg, Germany. **Lukas Krupp** is a doctoral student in machine learning for embedded systems at the Fraunhofer Institute for Microelectronic Circuits and Systems in Duisburg.



The internet is full of things

Pierre Gembaczka and Lukas Krupp

The devices, or “things,” that communicate and share data via the internet are part of a network that’s becoming increasingly connected.

It’s often the little things that make life easier. Think wearables, such as fitness trackers and smartwatches, or smart-home devices, such as lighting control systems, thermostats, robotic vacuum cleaners, and, of course, the voice-controlled, intelligent personal assistants that have already made their way into many living rooms. People may benefit from those and countless other devices every day, but few know exactly what’s behind them and how they work. This Quick Study pulls back the covers.

The internet of things (IoT) connects all small, intelligent systems that are already an integral part of many sectors in the global economy—from industry to agriculture. The IoT is the name of the network of physical objects equipped with sensors, software, or other technology that empowers them to exchange information with other objects. Such devices typically use microcontrollers for data processing to minimize cost and energy consumption. Most of them can even operate on battery power.

The IoT has its origins in the work of Kevin Ashton, who coined the term in 1999 during a presentation he gave as an assistant brand manager at Procter & Gamble. The company’s brown lipstick always seemed sold out to him even though it was still frequently available in stock. In the presentation, Ashton brought up the idea of placing RF identification tags on every product in the company in order to identify and track it through the supply chain. The IoT was conceived.

Today, it has become an enormous market, split into numerous specializations. Recent forecasts expect the IoT to grow from \$478.36 billion in 2022 to \$2465.26 billion in 2029. That’s on par with the value of today’s automotive-manufacturing industry worldwide.

Communication is the key

The IoT’s things are any devices that can be assigned an internet-protocol address and can transfer data wirelessly over a network. For direct communication between objects over short distances, consumer electronics technologies, such as Bluetooth and ZigBee, are common, especially in applications where data volume is low and little energy is consumed. For local-area networking and connecting multiple devices to the internet, Wi-Fi is a prominent example. Other technologies included in modern smartphones, such as near-field communication for short distances and cellular communication for global networking, are also common in IoT devices.

Automated information exchange between end devices, such as machines or central control units, is referred to as

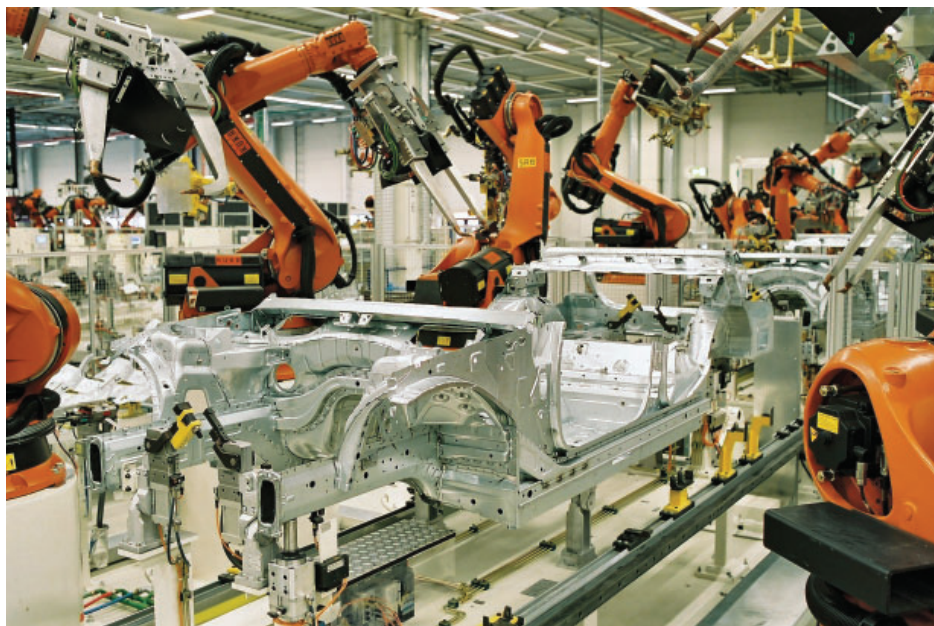
machine-to-machine communication. An example is the communication between robots completing a common task, such as assembling products. But it’s also possible to integrate a remote bank of computers, known as a cloud, to manage information from distributed devices in a central location. Several cloud service providers are now available, including Microsoft’s Azure IoT Hub and Amazon’s AWS IoT services.

Such IoT technology is perhaps most interesting to the industrial sector of the economy, in which the term industrial internet of things (IIoT) is now common parlance. In contrast to consumer-oriented devices, IIoT ones focus on industrially relevant applications. An example is the control of industrial robots in assembly lines awaiting sensor data to be sent to a controller before they can perform their task. Built into such control is a so-called deterministic latency, which allows a robot to react to its environment on time. Apart from such real-time constraints, many industrial applications operate in harsh conditions. Unlike a smart-home environment, in which the only information exchange may involve a few light switches, a smart factory, like the one shown here, may have dozens of machine parameters and sensor signals that must be constantly monitored and frequently processed.

Driven by the increasing distribution of IIoT devices throughout production plants, predictive maintenance and condition monitoring are the current trends in industrial fields. Thanks to that monitoring, companies can predict machine failures and defects in manufactured products at early stages—even before parts actually break. That’s an essential task in a smart factory, and it’s key to resource planning and process control. The multinational European aerospace company Airbus, for instance, has launched a digital-manufacturing initiative known as Factory of the Future as a way to increase its production capacity. To reduce errors and improve workplace safety, sensors are currently integrated into manufacturing tools and machines, and employees use wearable technologies, such as ecom’s smart eyeglasses Visor-Ex 01.

Machine learning

Machine learning (ML) algorithms, such as artificial neural networks, play an important part in the IoT. The huge number of sensors distributed in countless devices around the world and the increasing extent of networking between them generate a tremendous amount of data. Fortunately, ML methods are capable of analyzing that data to extract information and infer what’s going on. Voice-controlled assistance systems, for in-



stance, use ML to process and understand human speech. Likewise, sound-detection systems analyze environmental sounds, such as traffic on a highway, to interpret any detected patterns. (For ML applications to weather forecasting, see *PHYSICS TODAY*, May 2019, page 32.)

Two main approaches exist for designing a system architecture that integrates ML and the IoT. The first approach collects data in a central location such as a cloud server. Ordinarily, that data must first be transferred from the actual device before it can be processed. Unfortunately, such an enormous amount of data streaming from IoT devices to the cloud server consumes a lot of energy. What's more, any interruption to the connection may also cause the system to malfunction. To counter those potential problems, engineers have started migrating ML methods directly into IoT devices. The idea behind that second approach, which is now gaining increasing popularity, is to perform as much of the data processing as possible inside the particular IoT device at issue. And it dramatically reduces the amount of transmitted data.

The new generation of devices embodies a paradigm often described as the artificial intelligence of things (AIoT), which integrates the ML algorithms directly inside physical objects and products. The ML methods and algorithms that produce the integration are grouped under the terms TinyML or Edge AI. Devices that benefit from the local intelligence include surveillance cameras that do not require the transmission of raw images to a cloud server and autonomous robots in hostile environments that can detect and respond to threats all on their own.

High-performance hardware

Processing high volumes of data using ML requires enough computing power for the system to extract information and make a decision in a feasible amount of time. Specialized computing hardware, such as graphics processing units, can accelerate the data processing. Faster processing speed leads to lower energy requirements and ultimately an increased amount of data that can be processed. That capability supports outsourcing complex applications without the need for a permanent connection to a cloud server.

MACHINE-TO-MACHINE COMMUNICATION.

Robots coordinate when to fetch or screw together their components in this automobile assembly plant. They can autonomously schedule and optimize the assembling processes to minimize energy consumption and production time. Likewise, they can analyze their own condition using sensors embedded inside them and predict when they need maintenance or repair. (Courtesy of BMW Werk Leipzig/CC BY-SA 2.0 DE.)

New ways for robots to predict failures have emerged. Multiple high-speed data streams from cameras, microphones, and other sensors must be processed in parallel, such that the robots can understand their environment—by seeing through a camera, feeling through a pressure sensor, or hearing through a microphone.

What could the next generation of AIoT devices look like? One possibility is self-learning devices, such as wearables that can adapt to a

specific user or to an application. For large tasks, such as self-driving cars, several devices could even work and learn together (see the Quick Study by Colin McCormick, *PHYSICS TODAY*, July 2019, page 66). Bringing this vision to reality will require an ML framework that can run on arbitrary AIoT devices, handle training, and enable the integration of hardware-acceleration mechanisms for ML. Researchers at the Fraunhofer Institute for Microelectronic Circuits and Systems in Germany—where one of us (Krupp) studies—have already implemented that framework. Artificial Intelligence for Embedded Systems (AI4ES) is open source and developed in the C programming language so that it can run on any hardware.

For a sense of what a self-learning device could look like, consider Fraunhofer's smart power-sensor demonstrator (see www.ai4es.ai), which is used to monitor the condition of a machine. In many applications, the machine's current power consumption provides detailed information about its operation, energy efficiency, and maintenance requirements due to wear or damage. The sensor can be attached directly to the machine, and the different operating states can be trained. The sensor is configured via a smartphone or tablet connected by Bluetooth. So configured, the sensor does not have to constantly send data—and does so only when changes occur in the operating state. That saves energy, and there's little risk of communication failure.

Additional resources

- Fortune Business Insights, *Internet of Things (IoT) Market Size, Share & Covid-19 Impact Analysis, . . . , 2023–2030 summary* (2023), www.fortunebusinessinsights.com/industry-reports/internet-of-things-iot-market-100307.
- N. Dew, "Lipsticks and razorblades: How the Auto ID Center used pre-commitments to build the Internet of Things," PhD thesis, Naval Postgraduate School (2003).
- P. Jama, "The future of machine learning hardware," *Hacker-News* (3 September 2016).
- Fraunhofer Institute for Microelectronic Circuits and Systems, "Wireless Current Sensor for Condition Monitoring." **PT**