IOT authentication need

Picking the right security for the job is a challenging issue. Obviously, everyone wants maximum security for IoT solutions. But issues such as hardware limitations, cost consciousness, lack of security expertise, and more all play into which security option is ultimately chosen for how your IoT devices connect to the cloud. There are many [dimensions of IoT security](https://www.microsoft.com/en-us/research/publication/seven-properties-highly-secure-devices/) and in my experience authentication type tends to be the first one customers encounter, though all are important.

Strong IoT device authentication is required to ensure connected devices on the IoT can be trusted to be what they purport to be. Consequently, each IoT device needs a unique identity that can be authenticated when the device attempts to connect to a gateway or central server. With this unique ID in place, IT system administrators can track each device throughout its lifecycle, communicate securely with it, and prevent it from executing harmful processes. If a device exhibits unexpected behavior, administrators can simply revoke its privileges.

Whether it’s a sensor-based device or used to perform a specific function, all devices are open to hacking unless preventative measures are taken (we need to enforce security by design). There are several examples of this, from disabling a [surveillance monitor on a Turkish pipeline](http://www.homelandsecuritynewswire.com/dr20141217-2008-turkish-oil-pipeline-explosion-may-have-been-stuxnet-precursor) to attacks on medical devices such as [insulin pumps](http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm481968.htm) and [MRI machines](http://www.computerworld.com/article/2932371/cybercrime-hacking/medjack-hackers-hijacking-medical-devices-to-create-backdoors-in-hospital-networks.html). These attacks were potentially life-threatening and indicate that some hackers have no scruples when it comes to target selection or gaining bragging rights to fellow cybercriminals.



Authentication for the devices in IoT is different and considerably lighter weight than people authentication methods prevalent today due to the potential resource constraints of devices, the bandwidth of networks they operate within, and the nature of interaction with the devices.   
  
A lack of established industry standards for IoT authentication has led vendors to develop proprietary authentication methods. Since many IoT devices can be resource-constrained with low computing power and storage capacity, existing authentication methods are not a good candidate due to their significant bandwidth and computational requirements. There is a growing need to evaluate and streamline the methods adopted for device and service authentication over constrained IoT networks. It is important to analyze and use the factors essential for verifying the identity of ‘things’ to establish the desired level of trust in the device identity without overburdening the fit-for-purpose computing abilities of the IoT device.