Preserving Endpoint Device Security in the Internet of Things

Dr. Aasman was quoted in this article

Full Article at Analytics Week:

Device authentication is central to redressing the security issues that plague the IoT, some of which have eventually led to ***Distributed Denial of Service (DDoS)*** attacks. Another means of verifying endpoint devices is to leverage smart data approaches buttressed by semantic standards, in which devices are authenticated by the actual data emitted. According to ***Franz*** CEO Jans Aasman, “A lot of sensors already do emit as JSON objects. If they were JSON-LD objects then the identity of the sensor would be built into the signal.” JavaScript Object Notation Linked Data (JSON-LD) is a lightweight data interchange format dynamic enough to accommodate schema on read, yet useful for its linked data qualities in which its data objects can be connected to other objects on a semantic graph.

Using JSON-LD to describe sensor data is helpful for authenticating transmissions because of the richness of the descriptions and the unique identifiers native to the semantic graph technologies in which linked data works. “A sensor could have a unique I.D., obviously a URL,” Aasman noted. “And that’s just the sensor, but then the type of that sensor would be like a pressure sensor, and then we would have a taxonomy that describes what pressure sensors are.” With this approach, IoT data transmissions are verified by the actual data—and attributes—they contain.