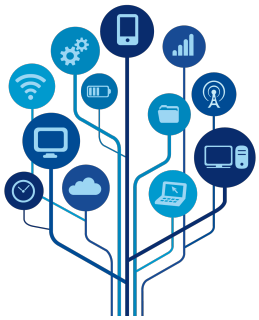
Securing IoT nodes in supply of chains

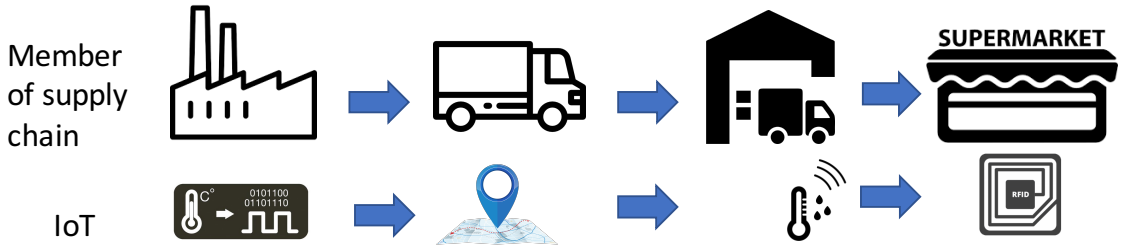


In the last few years, IoT devices popularity has skyrocketed due to the numerous benefits they offer. Essentially, they are handy for a lot of use cases where tough constraints are set, such as size (small devices) and connectivity (very well connected). These devices are a key part of the Internet of Things, where every device can take measures from the environment, perform actions and exchange data among other IoT devices. In spite of having much features, IoT devices lack high processing power as they are not intended to carry out expensive computations, rather they are small devices specially designed to carry out specific tasks; and usually they form part of an edge-fog-cloud architecture, where specific and real time computations are executed closer to the IoT devices. Moreover, the processes requiring high computation or storage capabilities are outsourced to fog or cloud servers.

In this scenario, IoT devices should interconnect as well as communicate with edge, fog and cloud resources. Internet's communications are mostly encrypted to provide protection and privacy. This protection consumes some of the available resources since every cryptographic task requires computational power and time to process it. Whenever IoT devices communicate among themselves, they must use a secure media which guarantees data privacy and integrity using cryptographic operations. What is more, in certain scenarios, such as supply chains where IoT devices have to be traced and monitored, such constraints lead to a stricter supervision.

SEN (Secure Edge Node) is an architecture able to maintain many IoT devices in contact while providing some guarantees like security, reliability and ubiquity. Likewise, these devices apply strict policies when communicating with themselves so every interaction remains authenticated and private. The proposed SEN architecture tackles security by design, determining how communications among IoT devices will take place and with whom. Using Blockchain as a baseline technology brings interesting functionalities such as ACLs (Access Control Lists) and fine-grain control of each SEN member. Whenever two IoT devices want to communicate among themselves, a specific code is run by the Blockchain that performs the necessary verifications (through policies) to ensure that communication is allowed between them. In case there is any issue, warnings are issued to the architecture so IT administrators become aware of them.

However, in some scenarios the communication between IoT devices should not be granted forever. We define as communication contexts, periods of time in which two IoT devices can communicate between themselves. This feature perfectly matches supply chains where IoT devices roam dynamically within different areas found in logistic scenarios, as it is shown in figure below, where a factory, a truck, a warehouse and a supermarket are member of supply chain. By restricting exchanges of data through communication contexts, SEN architecture always knows the conversations' history of the IoT devices. These contexts can be understood as "tickets"; in case two IoT devices own the same ticket and is approved by SEN architecture, thus making data exchanges to be possible only during ticket's lifetime.



On the other hand, as IoT devices can be added to SEN architecture, they can also be either disabled or removed. Malicious behaviors performed by IoT devices may be detected and warnings automatically generated through SEN's website. IT administrators can check at any given time the last generated warnings, the number of occurrences and which device created them and afterwards can act accordingly. In this case, the backbone Blockchain also allows disabling or permanently removing the detected IoT malicious nodes.