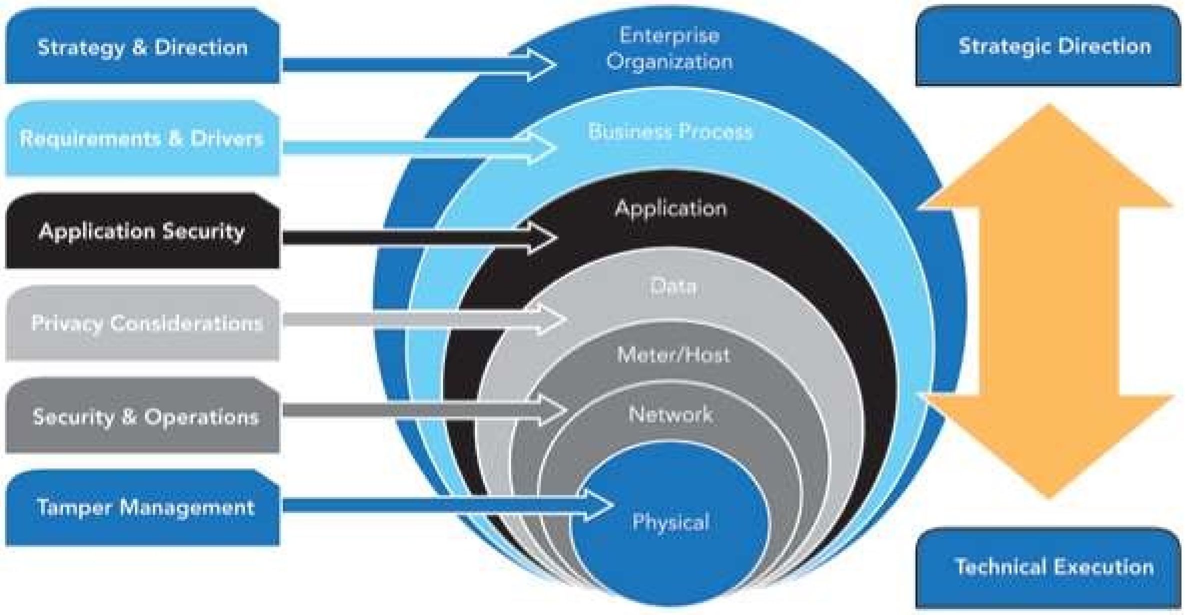
How to handle security in the IOT world - Tondo's layer model

The system provides security layers by design. Each connected product, gateway, and any 3rd party product that will connect to the ecosystem will include security elements to ensure that every single device in the field is securely accessed.

The following diagram represents the different layers of the system. From the security standpoint, the security strategy has to tackle every layer of the solution and make sure it is covered.



Here's how we address security in each of these layers - Physical, Network, Host, Data and Application:

- **Physical** – On the physical layer, the Cloud of Things security token / certificate is stored in an internal location of the Flash memory of the device. We are not using the MAC address as a token. A hacker would need to find a way to read the specific memory location to get the certificate or key. The key is unique to the device. If a hacker finds a way to read the key in one of the devices, he will not have access to the rest of the system limiting the potential damage he can make to that specific device scope.

- **Network** – The entire communication stack is based on TLS encryption ("advanced SSL") with certificate authentication. Since we control the entire communication stack, someone who wants to eavesdrop the communication packets will not be able to do it.

- **Meter/Host/Sensor** – The hub, oven and fridge have SSH-only access and will not have a login/password scheme. This will lead a hacker to have to gain access to the unique public key of the specific device. Even if a hacker gained access to this key, he will not be able to affect more than the scope of that device. (most of the latest IoT breaches happened when hackers used a common, “master user/password”, for a system. Such a key does not exist in our system).

- **Data** – The data for the system is stored in the IoT cloud (Microsoft, IBM, Google, Amazon). The security measures of protecting the data depend on the specific cloud that is used for IoT data storage. It’s important to note that no private information is stored in the IoT cloud. The identification of devices and hubs is stored as globally unique identifiers (GUIDs). The customer private information is stored in the internal customer’s ERP/CRM system that holds a link to the IoT identifiers. Thus, even if a hacker gained access to data in the cloud, he or she would not have access to the private information of customers.

- **Application** – The application has industry-standard security measures that prevent someone from the outside to gain access to the control dashboards – using methods that are used in web-based banking systems. Only users with the right credentials can use the system and the system is constantly monitored using the administrative authentication, authorization, monitoring and activity log:
    - Each person with administrative privileges to the system should be identified and authorized.
    - Administrators activities will be monitored and logged.
    - Administrative role management: each administrator or group of administrators (help-desk, system engineers etc.) will have different administrative rights such as view only, or remotely reset a device with prior approval of the connected product’s owner etc.
    - Some remote device control will not be enabled at all by design. For instance, there is no reason to remotely turn on a water tap as it may cause a flood. A water tap should be turned on only when someone’s physically present and operates it.