Ogauge Network Configuration

When designing an advanced IIoT device like Ogauge, there are several factors wich come into play. One has to think of the following :

- Mobile access (device configuration, registration, unclaim procedures)
- Telemetry data, which is one way
- Device control, which is two way (needs more security)

- OTA (over the air upgrade) for

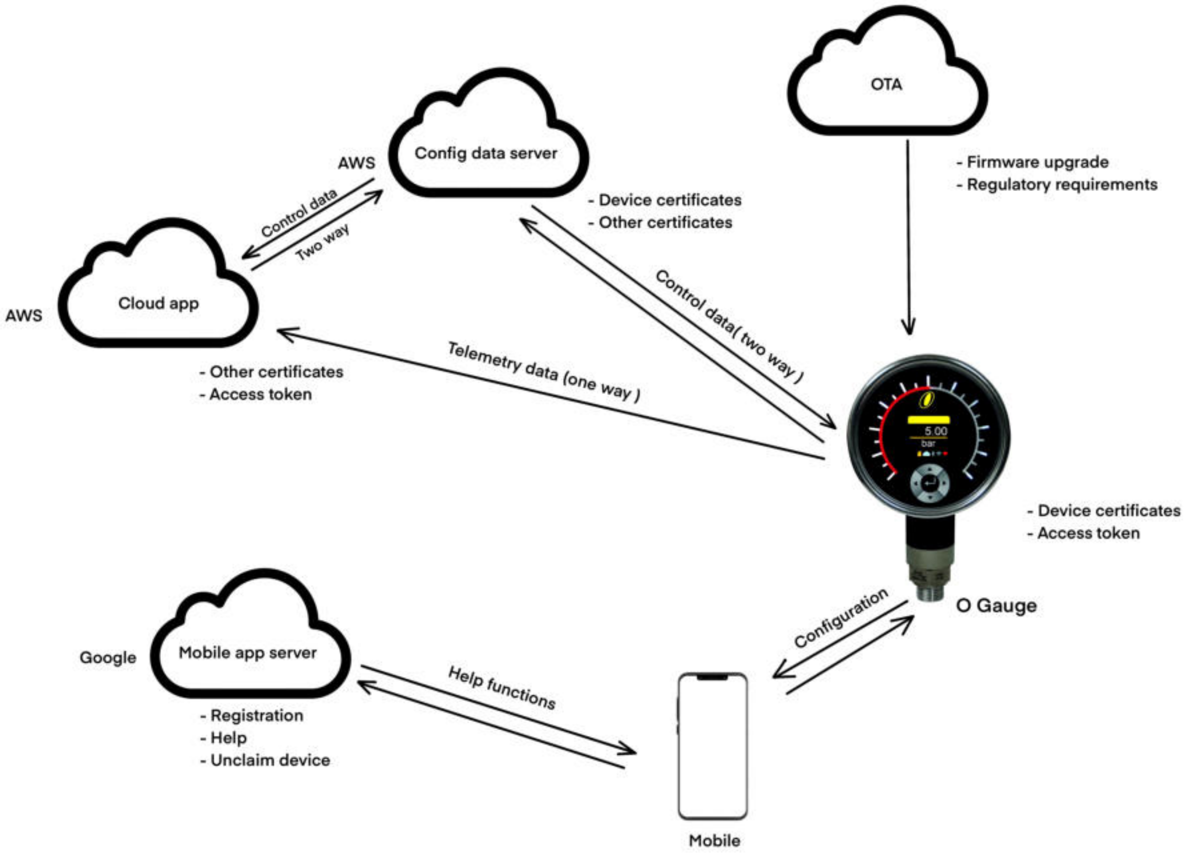
  - Firmware upgrade
  - regulatory requirements

- Help functions (forgot password, problems in use)

  - forgot password
  - problem resolution help
  - registration of gauge
  - unclaim device procedure

Internet access is needed for all of the above.

The general architecture of Ogauge is given in brief in the following picture :



It is possible that one has to use Ogauges inside a firewalled network. To safegaurd your network, we suggest to create a new subnet in your existing network.

A mobile application, is used for configuring the Ogauges, and also for any help and support functions. It is necessary that the mobile has internet access to **https://mapp.orion-instruments.io**

To ensure normal functioning of Ogauges, kindly keep the following endpoints and ports open on the subnet :

Sr.no	EndPoint	Outbound Port	Inbound Port
1	https://ogauge.orion-instruments.io	443	1883
2	mqtts://a1hwcg0rq9r5nn-ats.iot.ap-south-1.amazonaws.com	443	8883
3	http://ogauge.in	80	*

The mobile app will have the facility to set gateway IP, subnet mask and static IP (or DHCP).

For further clarifications, following points can be looked into by a third party :

Audit report
SOC – SIEM – logs inspection
SOC2/3 report from AWS
Region hosting
Encryption
Cloud app architecture
Role based access control

For any further clarification, please write to support@oguage.io