**3.1 Modbus and cyber-attacks**

1. Setup Modbus Client - Server architecture

The Modbus setup consists of a two-tier architecture in which a presentation layer or interface runs on a client, and a data layer or data structure gets stored on a server. In our case, the PLCs or RTUs are the client which send data or make requests to the server which is the Control Centre consisting of Master Terminal Units (MTUs).

The library used for this is the PyModbus v3.0.0, a full Modbus protocol implementation using twisted/tornado/asyncio for its asynchronous communications core. Since the library is written in python, it allows for easy scripting and/or integration into their existing solutions.

1. Encode data to Modbus format

Data encoded in the Modbus format contains various headers and protocol syntax requirements to enable it to be transmitted over the internet in the form of Modbus Payload. This can be achieved using the PyModbus library and its built-in functions to encode and decode the data and its corresponding payload.

This encoded payload is sent from the client to the server over the internet and stored in the holding registers. The client then sends a GET or Fetch request to the server and receives the encoded data from the database. This is payload is then finally decoded back to raw data using PyModbus.

1. Setup cyber-attack architecture

The cyber-attack architecture consists of three machines, real or virtual. A communication is established between two of the devices over the internet via the Modbus protocol. A third machine will perform the cyber-attack by inserting itself in between the other two in such a way that all the communication is routed through it.

1. Perform Man-in-the-middle attacks

A MITM attack was performed with an Ettercap tool that maliciously modified the Modbus TCP commands between the Master and PLC workstations. Weaknesses of the Modbus TCP that were targeted by the Ettercap tool involved sending commands in clear text and lack of authentication within the Modbus TCP protocol. The Attacker workstation then uses the MAC addresses provided by the Ettercap scan for a MITM with ARP poisoning (ARP spoofing) to send falsified ARP messages. The ARP spoofing results in the linking of the attacker’s MAC address with the IP address of a legitimate computer or server on the network.

1. Gather cyber-attack data

Generate and gather the data produced from conducting cyber-attacks on the network. Perform data wrangling, feature extraction, etc on the gathered data to prepare it for the machine learning model.