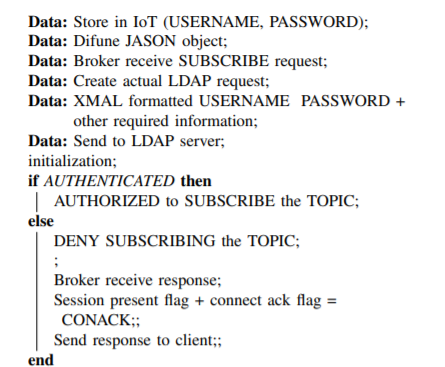
Make an authentication platform employing MQTT V5.0 and LDAP with efficient data and time synchronized transmission for IoT environment.

Flow.



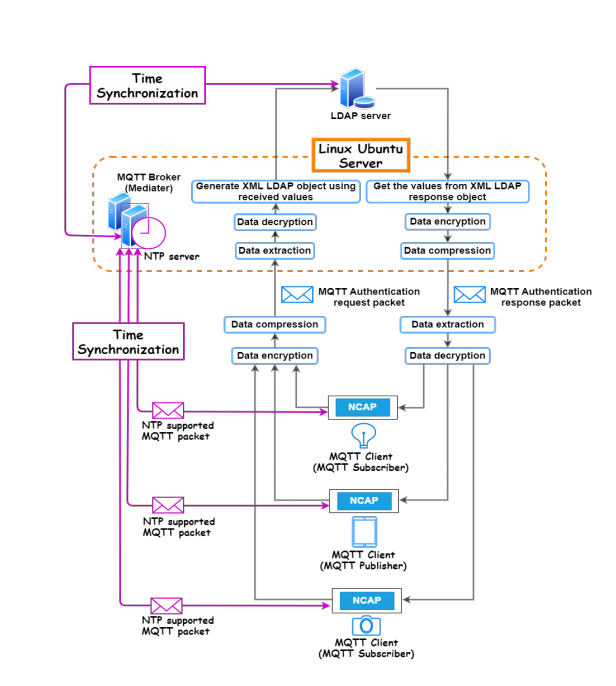
The AUTH packet is then altered by adding the LDAP request parameters to the payload field in this AUTH packet as a JSON object. Default JSON message is a key-value pair. In here transmit only the values except the keys. The modified MQTT packet will be referred as MQTT authentication request packet.

the values in this MQTT authentication request packet will be sent to the MQTT Broker as a bit stream. Then the MQTT Broker will acknowledge and send a response to the MQTT client to indicate the receiving of this packet

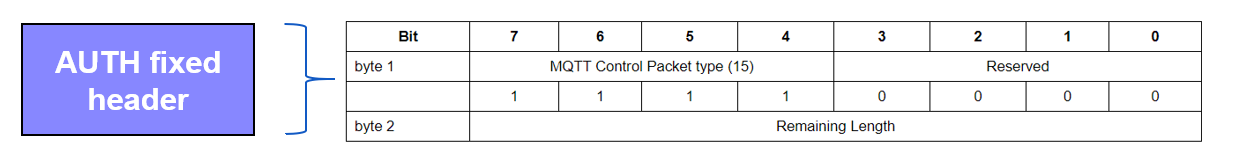
NCAP processor to get the computational power which need to do the securing the MQTT packet, which contains the authentication parameters required by the LDAP authentication server. This will be achieved by using hashing. Hence, in order to communicate with the MQTT Broker without making the IoT communication network busy and to avoid bulky messages, the packet will be compressed using GZip

process the MQTT message at the MQTT broker to support LDAP. Tasks;

* LDAP server should be configured with all the IoT devices, subscribers and access controls
* IoT devices should be registered with username and password
* Credentials should be stored in the DB of the LDAP server
* Messages from non-authenticated devices should be dropped at the broker/deny access



* Creating the LDAP Authentication parameters and Alter the basic MQTT message
* Generating MQTT packets using NCAP. Compression of the encrypted authentication request using G-ZIP compression
* Process the MQTT message at the intermediary device to being the bridge among the IoT device and the LDAP server
* **Main objective**
* Altering the basic MQTT message by creating LDAP authentication parameters in order to proceed with the LDAP authentication.
  + 1. Exchanging MQTT Authentication packet with the MQTT Broker and embedding the Authentication parameters.
  + 2.    To include time synchronization during the data transmission.



Text

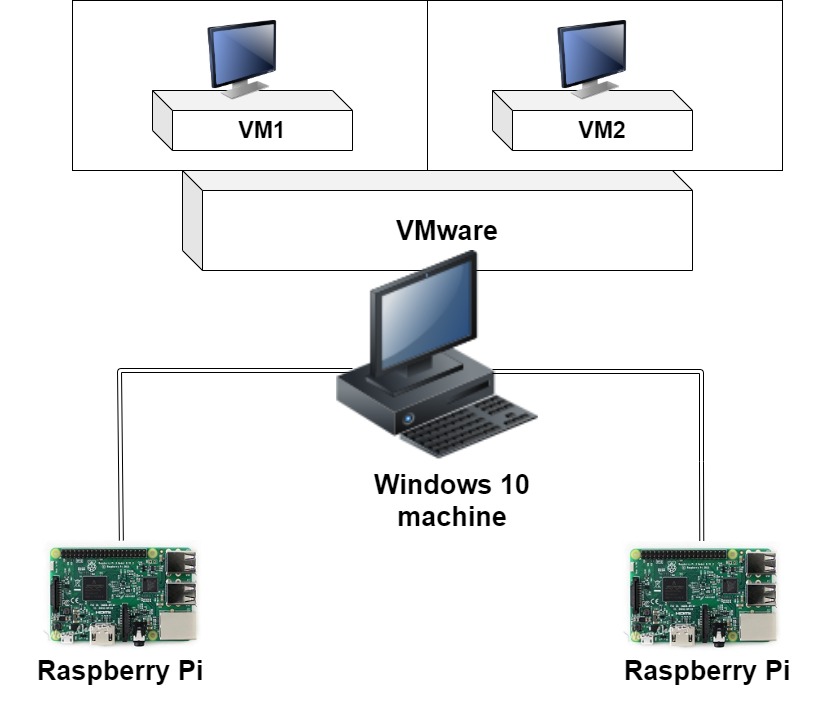
Description automatically generated

Text

Description automatically generated

Auth function which is located in the Auth.py python file of the MQTT V5 client.

* Generating MQTT packets using NCAP and compression of the encrypted authentication request using G-ZIP compression.
  + Securing authentication parameters and communication of the packets.
  + Optimizing the resource consumption



MQTT Broker

MQTT Clients

Graphical user interface, text, application

Description automatically generated

Up now I have tried using this method to hash the hardcoded password.

Expected task

* Embed the python code to the auth function
* Write a function for compress and de-compress

Text

Description automatically generated

In here the created auth packet will be unpack in the broker side.

* Process the MQTT message at the intermediary device to be the bridge among the IoT device and the LDAP server.
  + To verify IoT devices
  + Define policies for authorization of the IoT publisher & subscriber

Text

Description automatically generated

This will generate a LDAP request in the broker side

Expected Tasks

* Extract the authentication parameters from the received packet
* Define the auth plugin
* Complete the actual LDAP request