**Device Manufacturer Initial Firmware Flashing**

When the IOT device manufacturers flashing the firmware into the IOT device’s ROM chip, we add a signature generation step to create a unique firmware signature to every flashed firmware copy. This signature verification feature will avoid the attacker to create a fake IOT device and connect to our server even he has got the IOT firmware sample, the firmware flashing program or an unused IOT device (such as an old sensor which was not used anymore).

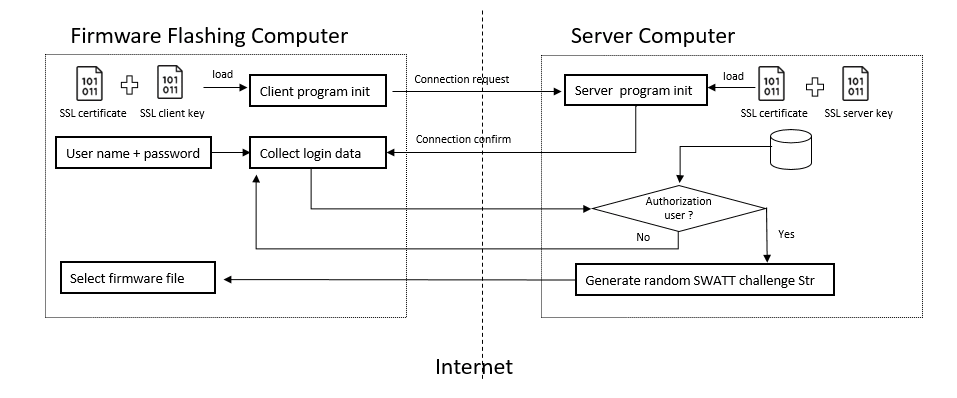
The firmware flashing program contains two parts of program (client and server):

1. Firmware flashing client: The client program (running on device manufacturer’s computer) is used to login server, generate the IOT device signature, flash firmware and server signature to IOT device ROM chip.
2. Firmware verification server: The server program (running on the IOT server) is used to record the IOT flash information to the database. Verify the IOT device registration.

There are three steps to finish the firmware flashing initialization and the client-server communication is using SSL/TLS.

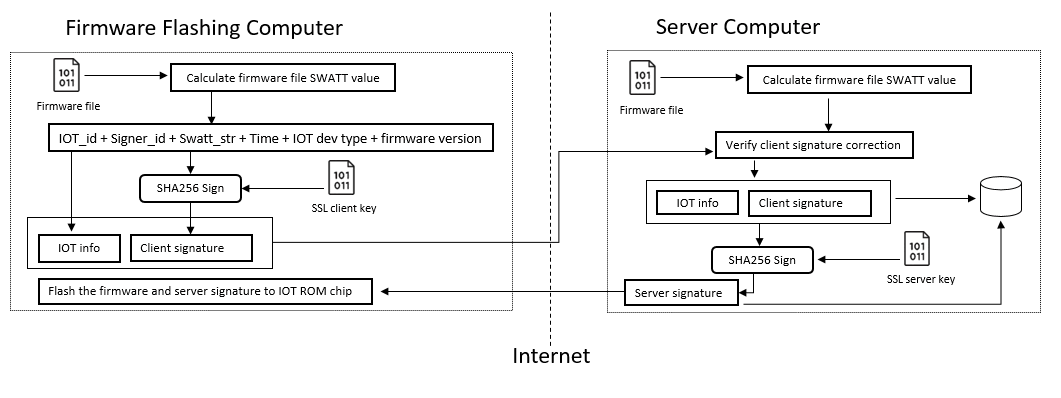
Step 1: System initialization and client login

The user needs a valid username and password to start to use the IOT firmware flashing program. Otherwise the user cannot use the program’s firmware flashing function. After the user name and password has been verified, the server will send a random SWATT challenge string to client and the client firmware selection function will be enabled. (The program execution flow is shown in the Figure below)



Step 2: Client signature generation and server signature deploy

After the manufacturer select the firmware file, the client program will calculate the file’s SWATT value based on the received SWATT challenge string. The server will also do the same SWATT value calculation for the further verification. Then the client will package the IOT device information (IOT\_id + Signer\_id + Swatt\_str + Time + IOT dev type + firmware version) and use client’s SSL key to sign it to get the client signature. The IOT device information and client signature will be sent to the server part. After the server has verified the client’s SWATT value and the client signature, the server will use its SSL key to sign the whole message (IOT\_id + Signer\_id + Swatt\_str + Time + IOT dev type + firmware version+ client signature) to get the server signature. The server signature will send back to the firmware flashing program and flashed with the firmware into the IOT device’s ROM chip. At the server part the IOT device information, client signature and the server signature will be saved in the data base. (The program execution flow is shown in the Figure below)



Step3: IOT device verification

When the IOT device try to connect to the server, it loads the server signature from the ROM and send it with the IOT device information to the IOT server. If all these data can match the record in the server’s data base. Then the IOT device’s data will be accepted by the server.