If after entering a _invalid_ username and password

Client selects _no_ for signup.

Retry.

OR a invalid password was given for a known user.

auth()

Ask and assign the privilege level

then **RETURN** to handle()

signup()

handle()

Before authentication

After authentication

First get a memory spaces to read and write

get_db()

GET()

Second keep processing GET and POST request

while length 0 data is not sent by client.

if GET request

if PUT request

PUT()

: Member function of **AuthTCPServer** class

: Member function of **GET_PUT_TCPHandler** class

:Code from the function from where the arrow come(in this case from handle())

EXECUTION FLOW

A connect request from client will trigger the handle() function.

Authentication will take place by calling auth().

After authentication we will have a username and its privilege level.

lvl : usertype
0   : manager
1   : user(non-manger)
2   : guest

Use the username and privilege level to get the space client can read and write.

After getting the space keep processing GET and PUT requests while the client doesn't send length 0 data.