I intend to create a P2S(Peer to Server) Chat system, which will allow text chat over TCP.

C# provides us with a HttpListener method and WebRequest method, then latter will be used to create and send Guest requests over TCP and the prior would allow for the listening and handling of GET requests on the server.

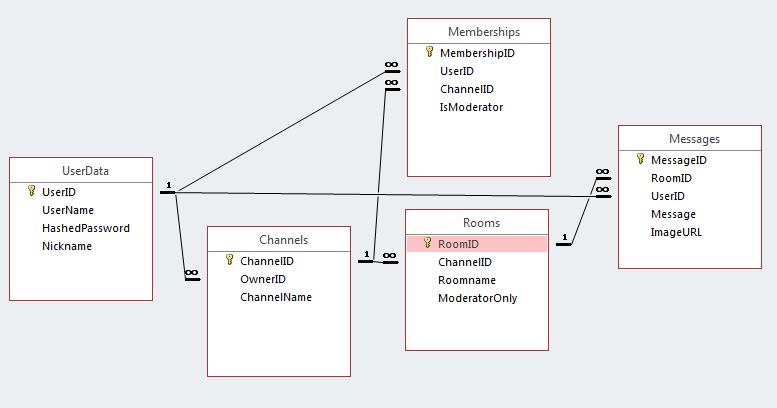
Headers will be used inside of the GET request with non-encrypted Keys and encrypted Values and will always contain an Instruction number to indicate the requested operation and then any data associated with the request,  
Response data will be sent in the format of a json which will always contain a Success Boolean and a Message string to indicate if the request was a success and if not, what went wrong.

I am uncertain at this time what encryption method to use, but I am set on using a symmetric key which will be exchanged via Diffie-Helman in order to keep the key relatively secure.  
The initial Diffie-Helman requests will be unencrypted as it is not necessary for the exchange method.

All data will be stored in an SQL database (example structure at bottom).

User passwords will be hashed by the user before it is sent and will be stored encrypted using itself as the key(so that if the database is breached the hash cannot be known),  
to validate if a provided hashed password is correct the stored encrypted hash will be decrypted using the provided hash as the key, if the decrypted hash and provided hash now match, the user is authenticated.  
All other user data (except usernames) will be stored in an encrypted form, using the hashed password as its key.  
Data such as messages and room data will be stored unencrypted, as encrypted storage of this information Is not necessary and may slow down and complicate the process.

I intend for users to create rooms which may have an infinite amount of users and an infinite amount of messages in them.  
The owner of the room has the ability to add administrators, who will (along with the owner) have the power to add and remove users, remove messages.  
Each user may join a limited amount (10?) of rooms at once, and may have an infinite amount of direct messages with other users.  
I may also add the ability to share images.



I aim to appeal to groups with low technical ability and who prefer programs with simple and easy to use layouts. Like the elderly and other more technologically inept groups.

In order to test the simplicity of the program I will have my grandparents use it, as they have a limited technological knowledge and should be a fair test of its usability.