

New social network system – A revolution

This paper is a update to that I wrote in 2017: [decentralised social network system](#)

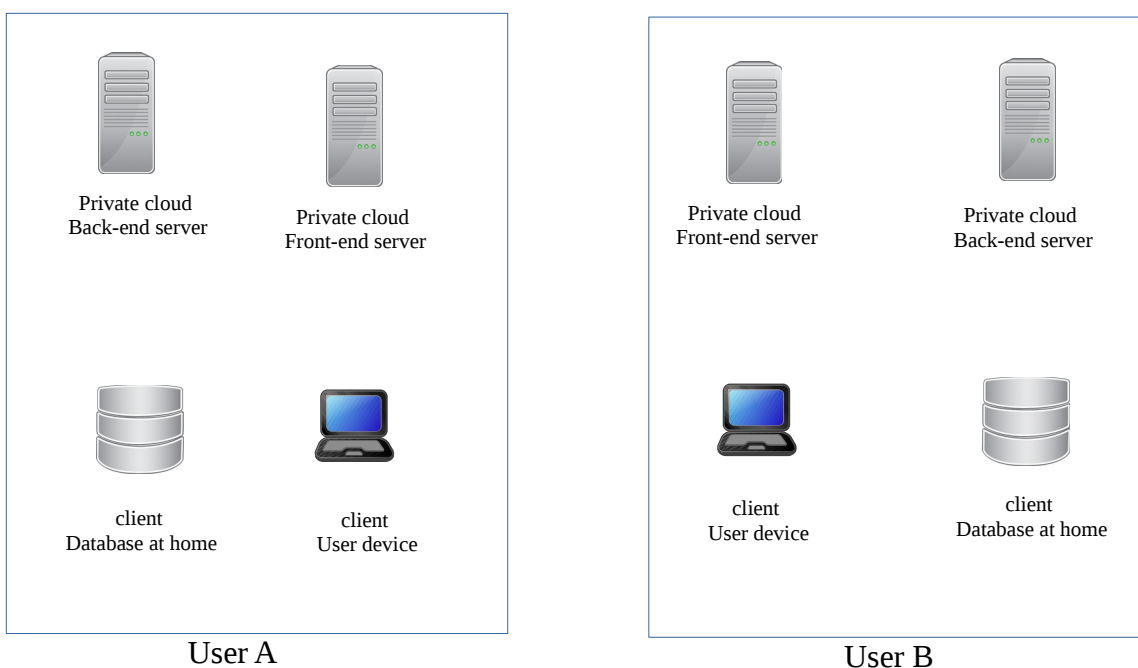
Free flow of information is very important, it can save lives, if people in China had the option to flow information freely, people all over the world would already knew the COVI19 virus at the very beginning! Doctor Li Wen Liang tried to warn his relatives in a small chat group with the out break of the virus, shortly after that he was arrested for sending rumors! He is certainly one of the people in China who knew the information in the early stage, others keep silent because of they knew the big brother is watching their chat App. If only people in China had the option to choose a chat App which can overcome the Chinese Communist Party's censorship, more people could had set the alarm before Li Wen Liang! Sadly no one in China has the option so far! Tragically many many people suffering the lost of their families,relatives and friends because of that, in China only, the number is huge, but still kept confidential!

I was raised up in China, where almost every information on media is censored,so I know how terrible the consequence of brainwash is ! I know how terrible people would behave under brainwash! It is an end to human civilization ! China used to have good culture, people used to behaves more decent, but now good thing are dying out there, it has been becoming a jungle of animal world !

Freedom is not free, but free things always come at a heavy cost of freedom! That is the problem of free chat apps I am talking about !

For today's technology, we have all the necessary wheels to build a website of our own that can talk to each other ! It is just that simple : connect your website to other's, and you connect to the world. Why should people spend countless time on other's chat app, while letting your own website looks like a dull fish !

Below is an architecture of the system :



➤ Private cloud Front-end server

modern SPA (Single Page Application) website use REST framework, for personal use situation front-end server can be deployed together with back-end server on the same VPS.

➤ Private cloud Back-end server

Backend of REST framework . mainly do signaling between peers and store database that is intended for public access . It connects to other users via websocket for long connection, handle the get request while other user following your post or other section updates, or post request when other user wants to write a comment or something under your post.

When connecting to other users via websocket, it is necessary to use the standard handshaking protocol, fortunately it is not complicate, we can borrow the idea from ip/ethernet protocol, but in Json format for application :

| Key words | Value | Encryption/decryption |
|-----------|--|---|
| from | { "ip": "xx.xx.xx.xx", port: 8080, username: "someone" } | Standard https, private and public key pair between peer and signal(backend) server |
| to | { "ip": "xx.xx.xx.xx", port: 8080, username: "someone" } | Standard https, private and public key pair between peer and signal(backend) server. When the ip != my ip, encrypt the package and forward to the destination ip, if you choose to server as an relay from one of your friends to another. |
| type | Operation type | Standard https, private and public key pair between peer and signal(backend) server |
| data | P2p data, | Peer to peer customized private and public key pair |

➤ Client database at home

nowadays trust is more valuable than gold, but network is build based on untrusted system,so it is necessary to store your private data, like chat log, in your own place, like a small device at home, serving as database. the level of security depends on how much money you are willing to spend on your database device, and how important for others to hack, there is no absolute safe system, but it is far more better to hand over all your private data to big companies as training data for free ! In that way, these companies probably know you better than your spouse! There is a saying in Chinese: 無知者無畏, which means when you don't know nothing about danger, you are very brave! Not just in China, with current chap apps, we are all chatting with each other like a group of people running naked. When do people come to realize that I do need to cover my private spot ???!!!

This database connects to backend server as a websocket client, and via private protocol since it only talks to your own backend server.

- client user device
could be browser / customized app on laptop or smart phone. It connects to front-end server. If the client device behind NAT does not support webrtc peer to peer, it falls back to use his own backend server as a relay!
- ICE server, even though Google provides a lot of free ICE server, but in situation like China, most of Google's IP address has been blocked by the nasty Great Fire Wall, which sensors all the information going out and in China, we could deploy opensource TURN (traversal using relay NAT) on our own backend server, but we need to alter the code, because TURN server require 2 static IP, while our backend server mostly has only one ip address, to overcome this, we can ask the database server at home to send a request to the client device, if the client device can receive, then we know it sits behind a NAT that can works as real peer to peer, otherwise, the client device need to fall back to use his own backend server as relay to use webrtc.

https://github.com/brianwchh/decentralized-social-networking-software-system_1/blob/master/a%20decentralised%20social%20networking%20software%20system%20for%20freedom%20network.pdf

https://github.com/brianwchh/decentralized-social-networking-software-system_1