Uporedna analiza Chat aplikacija. Eksperimentalno testiranje da li su direktne ili je komunikacija preko posrednika. Zanimljivosti vezane za Chat aplikacije I njihova primena u borbi protiv svih oblika kriminala.

Analiza Chat aplikacija:

**Direktna komunikacija (P2P, Peer-to-peer)**

Korisnici direktno komuniciraju jedni sa drugima bez centralizovanog servera. Poruke se salju preko TCP ili UDP konekcija koje se uspostavljaju medju klijentima. Svaki kompjuter se ponasa I kao klijent I kao server.

+ Nema centralne tacke oktaza (server ne mora da cuva podatke).

+ Veca privatnost – poruke ne prolaze kroz nekog posrednika.

+ Moguca manja latencija (kasnjenje) kod lokalnih mreza.

- Nema centralizovanog upravljanja pa je bezbednost manja.

- Nema istorije poruka ako se ne cuvaju lokalno.

Primer: Skype, WhatsApp (za pozive I video pozive)

**Komunikacija preko posrednika (Server-Client)**

Svi klijenti se povezuju na centralni server koji prima, obradjuje I prosledjuje opruke drugim klijentima.

+ Jednostavnija sinhronizacija I upravljanje korisnicima.

+ Moguce snimanje I istorija poruka.

+ Kontrola bezbednosti I autentifikacije.

- Centralna tacka otkaza (ako server padne, niko ne moze da komunicira)

- Server moze da ima uvid u **sve** poruke, manja privatnost.

Primer: WhatsApp, Discord, Slack, Telegram, Facebook Messenger

Postoje I hibridna resenja koje koriste oba pristupa tako sto imaju centralizovani server za logovanje, dok se poruke salju direktno izmedju klijenata (E2E enkripcija, End-to-end).

Uglavnom je **privatnost najbitnija** pa je prioritet da postoji E2E enkripcija, te je direktna veza bolja ali I slozenija.

Chat aplikacije mogu itekako da pomognu u svakodnevnoj borbi protiv kriminala. Poput komunikacije izmedju raznih sluzbi u realnom vremenu, brza I sigurna razmena podataka o lokacijama sa incidentima I osumnjicenima.

Sa druge strane mogu I da budu zloupotrebljene pa kriminalci koriste ekriptovane chat aplikacije za neke ilegalne dogovore, kupoprodaju I sta sve ne.. Pomoc bi bila da sve poruke sadrze metapodatke koje ce cuvati podatke naprimer o vremenu slanja i IP adrese.

Dorada resenja:

Trenutno se poruke cuvaju unutar klase ChatRoomHistory -> LinkedList<RPCRoomChatMessage> messages

Resenje bi bilo da se poruke ne cuvaju na serveru kao do sad, vec da sami korisnici lokalno skladiste svoje poruke I da se poruke prosledjuju svim korisnicima u realnom vremenu (Peer-to-peer komunikacija). Server bi mogao da ostane u sluzbi cuvanja informacija o korisnicima I raznim grupama tj u nasem slucaju sobama. To bi bio Hibridno resenje koje sam prethodno pomenuo. Prednost bi bila postignuta privatnost, tj da server ne zna sadrzaje poruka. Mana bi bila da ne bi postojala mogucnost getLastMessages() jer server tada ne bi cuvao poruke kao I gubitak poruka ako korisnik nije bio aktivan. Implementacija peer-to-peer komunikacije nije toliko jednostavna zbog vise stvari:  
- Nat I firewall ogranicenja, vecina korisnika je iza rutera ili firewall-a sto otezava direktno uspostavljanje veze izmedju klijenata.

-Potrebna inicijalna detekcija I povezivanje peer-ova a bez centralnog servera je tesko otkriti IP adrese I portove aktivnih korisnika. (peer discovery problem)

- Odrzavanje stabilnosti mreze u P2P sistemima korisnici cesto dolaze I odlaze.

- Manja je bezbednost I autentifikacija pa je teze proveriti identitet ucesnika u konverzaciji.

Literatura:

1. <https://www.cometchat.com/blog/peer-to-peer-chat>
2. <https://www.reddit.com/r/rust/comments/zsrll2/trying_to_build_a_peertopeer_chat_app_would_love/>