Software System Lab - Project

FastChat

Chaitanya Garg (210050039)
Jennisha Agrawal (210050074)
Atharv Kshirsagar (210050025)

Telepound

Database

Database has 3 tables.

- clientinfo -

Column name	data type	details
username	text	unique id
password	text	strong password
public_n	text	pubic key n value
public_e	text	pubic key e value
private_d	text	private key d value
private_p	text	private key p value
private_q	text	private key q value
salt	text	salt to encrypt keys

Database

- undelivered -

Column name	data type	details
time	double precision	time of sending message
touser	text	user message is directed to
message	text	message to be sent

- groupinfo -

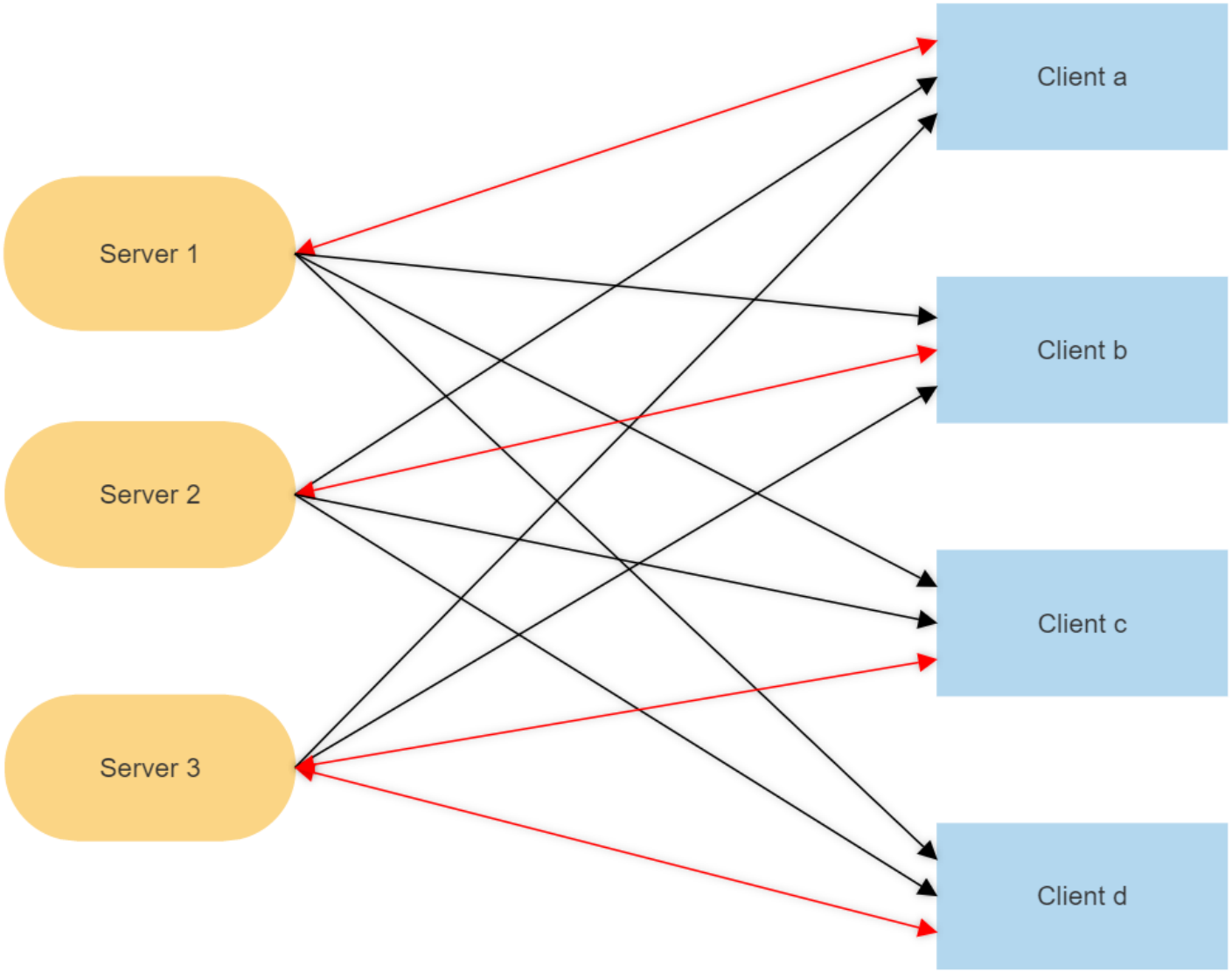
Column name	data type	details
groupname	text	The name of group, unique id
admin	text	The username of group admin/creator
members	text[ ]	username of all group members

- Database has two roles :
  - Postgres(default) : Role for server and load balancer, has all privileges.
  - Client : Role for client, can only select information.

Login and Sign-Up

- Authorization happens in client itself.
- Sign-Up
  - Checks if username already exits
  - If username is new then sign-up request request is sent to load balancer which stores new users in database
- login
  - Checks if given credentials are correct
  - Maximum 5 incorrect attempts are allowed
  - If correct login requests is sent to load balancer which stores new users in database
- Load balancer sends a assigned server and list of all servers to the client
- Client connects to all server

Multiple Servers



Load Balancing

- Load Balancer maintains a priority queue of servers based on some load factors
- During login/sign-up load balancer assigns server with least load factor at the time to the clients.
- Client can receive messages from all servers but can send messages only to assigned server.
- After every fixed number of messages, request to assign new server is sent to load balancer (number of messages can be varied to optimize performance)
- When new server connects , its information is sent to every client and they all connects to the server

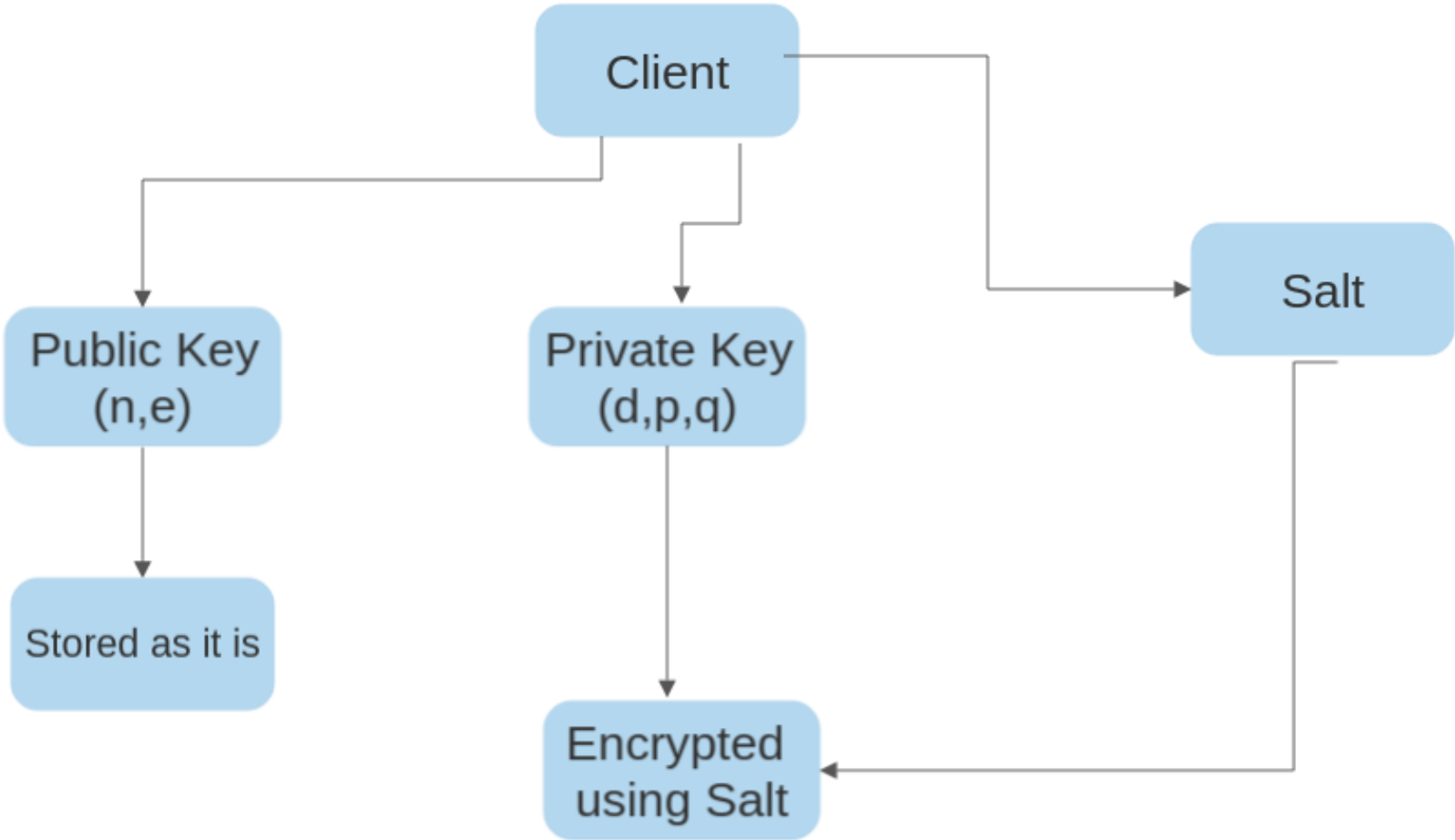
Sending Messages

- All communications is through json objects.
- Read receipt are sent to message sender.

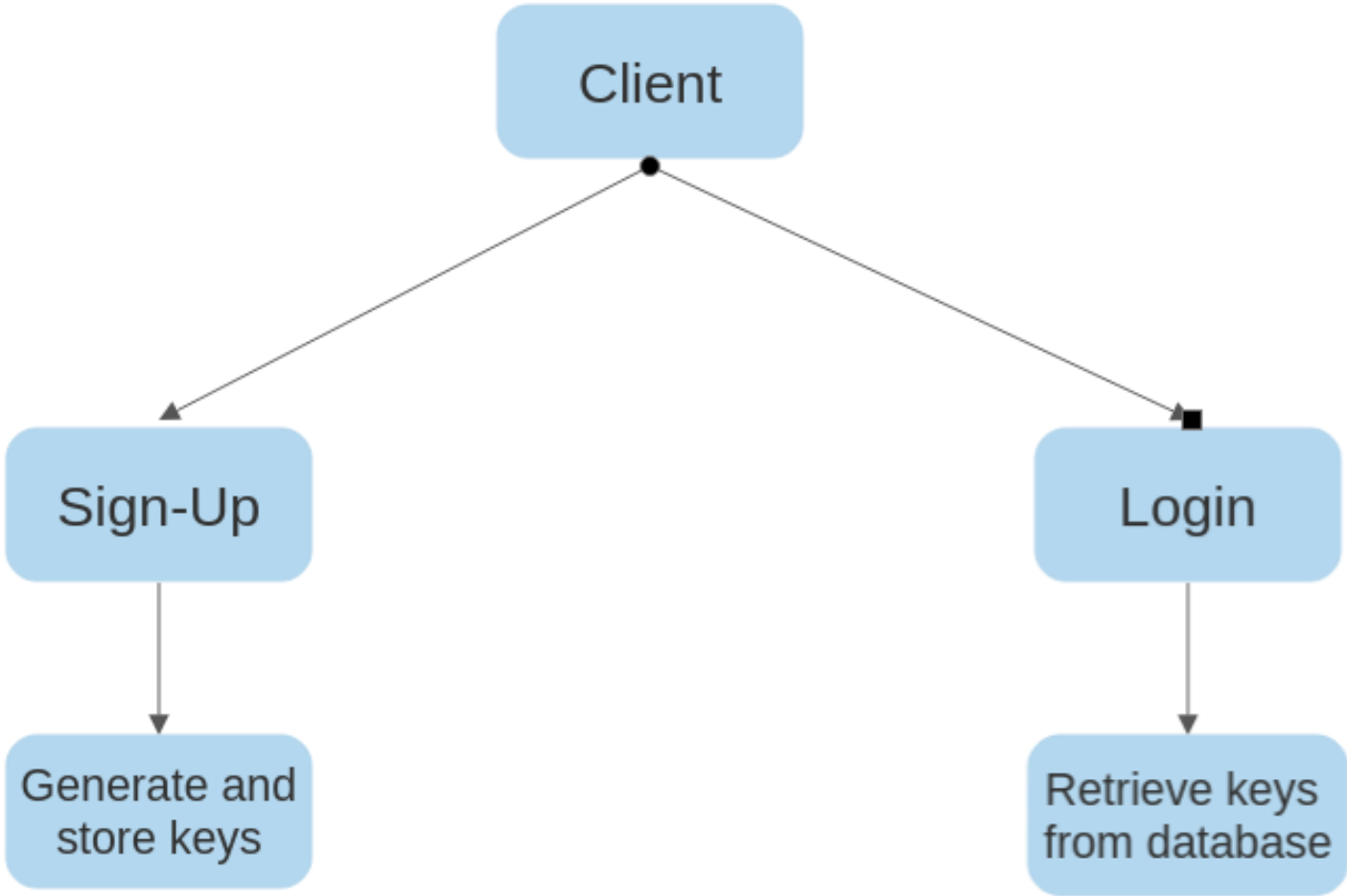
Storing messages for offline clients

- If the recipient is offline then the message is stored in the undelivered table of database.
- When a user logins all of its undelivered message are retrieved and sent to it.

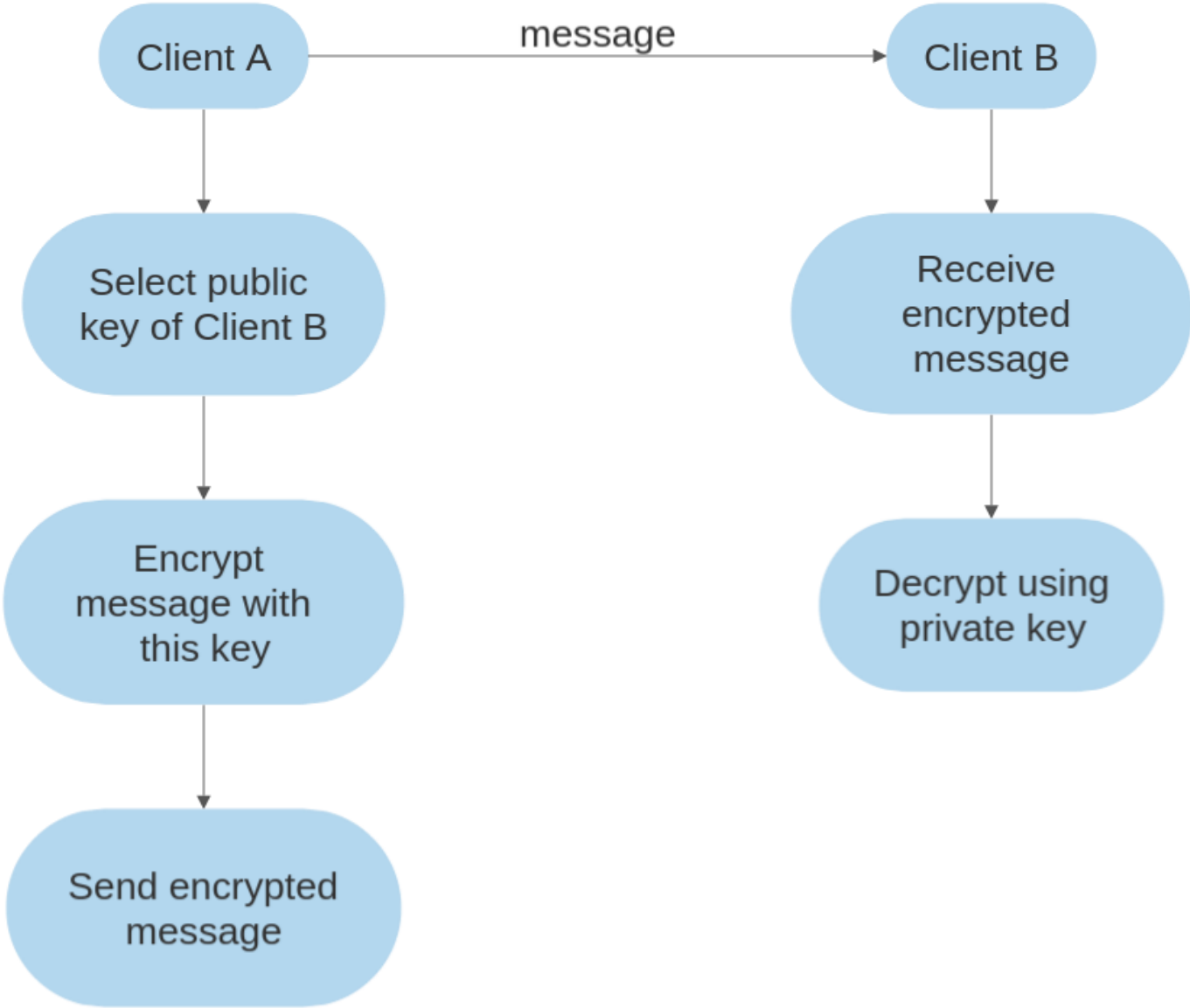
Encryption


Client
Public Key
(n,e)
Private Key
(d,p,q)
Salt
Stored as it is
Encrypted
using Salt

Encryption


Client
Sign-Up
Login
Generate and store keys
Retrieve keys from database

Encryption


Client A
message
Client B
Select public key of Client B
Receive encrypted message
Encrypt message with this key
Decrypt using private key
Send encrypted message

Group Chat

- Some commands are preserved as keywords, ('CREATE GROUP', 'ADD MEMBER', 'REMOVE MEMBER', 'LEAVE GROUP')
- The Group Name is also a unique id. Meaning username and groupname, combined, are unique.
- On Creating group, A group, with only 1 user is created and stored in the groupinfo table.
- This user is the admin, and he can add remove members by using ADD MEMBER, REMOVE MEMBER command.
- Group Messages are encrypted individually for all members.
- Any member can leave group using Leave Group command.
- If the group admin Leaves the group, or removes himself, then the group is deleted.