★ VM → Virtual Machine
  ↳ per one acc 1 VM ; extra purchasing erases
                    existing data.

Cloud Storage:
  ↳ centralised extensive storage
  ↳ offers security using

  (a) Encryption: data is stored as cyphertext
      i.e. unreadable data → 3rd party
      cannot access.
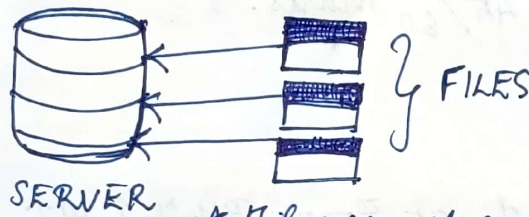
SERVER

FILES

Components:
a) SERVER (platform)
b) OWNER
c) USER

★ Files are stored using
  security key generated by the server.

USERS only view the unreadable content as 0, 1
  ↳ needs to request the server for access

Keys: (i) Private (ii) Public (iii) Secret (iv) Trapdoor

★ LOAD BALANCE: checking server performance using
  values such as α, β, γ

  (b) Decryption: encrypted data is restored
      back into accessible format

    Encryption   vs.   Decryption
• into ciphertext   • into plain text
• secret (or) ~~private~~ public key   • decrypted using
  is used.   secret (or) private key.
• Appl.: E-mail security,   • Appl.: WhatsApp
  OL banking, Data   Messaging, HTTPS websites.
  Storage

(i) Private: Symmetric key encryption
(ii) Public: Asymmetric, involves pair of keys.
(iii) Secret:
(iv) Trapdoor: Only works one way. needs special info
     for the other way.