1. Co-tenancy is a crucial characteristic that sets cloud security apart from conventional computer security. Co-tenancy involves everyone using the same network that the cloud service provider has given, including possible attackers. Attackers now have more options to conduct side-channel attacks, jeopardising the safety of other network users. This is in sharp contrast to traditional computer security, which places users in their own segregated networks, making it nearly hard for an intruder to get access unless specifically authorised. Co-tenancy, a feature of cloud security, essentially allows for the presence of attackers on the same network as authorised users, opening up security gaps that are not generally present in conventional computer security setups. This crucial distinction highlights the fact that special considerations and precautions are needed for cloud security.

2. Scenario 1: In this case considering Nozama as a potential Attacker, below are the reasons as follows,
   Data that is kept on their servers can be accessed by Nozama. Employees or administrators at Nozama may in some circumstances abuse their privileged access to obtain unauthorised access to confidential documents. When entrusting third-party service providers with sensitive data, this insider danger is a prevalent worry.
   It's critical to look into Nozama's history of data breaches and security concerns. It may be reasonable to question Nozama's suitability as a service provider if they have a track record of security flaws or previous breaches. Past occurrences may suggest a higher chance of malice intention.

   Scenario 2: In this case considering Nozama as not a potential attacker, below are the reasons as follows,
   As a trustworthy cloud service provider, Nozama probably adheres to strict security procedures, regulatory requirements, and compliance norms. They are less likely to engage in malevolent behaviour since they have a stake in upholding their good name and customers' confidence.
   To protect the stored data, Nozama may use effective encryption methods and security controls. Even their own staff may find it extremely difficult as a result to access sensitive papers without the necessary authorization. The claim that they would behave as attackers can be refuted by their dedication to data protection.

3. When choosing Elgoog cloud service there are several advantages over local in house data several but there are also some disadvantages. Lets discuss below

   Advantages of using Elgoog cloud-based storage service:
   - Organisations do not need to manage server maintenance, such as hardware upkeep and software updates, because the cloud provider handles these responsibilities.
   - Cloud storage allows for the simple adjustment of storage capacity as needed, resulting in cost effectiveness and responsiveness to shifting storage requirements.
   - The capacity to access cloud-based data from any location in the world improves remote work skills, fosters collaboration, and guarantees data availability.

- Cloud service providers typically offer robust backup and disaster recovery solutions, reducing the risk of data loss and ensuring data integrity.

Disadvantages of using Elgoog cloud-based storage service:

- Due to the shared network and infrastructure between authorised users and prospective attackers, cloud storage creates security issues. Because of this, there are hazards from data breaches and unauthorised access.
- While local servers can be used even when there is no internet connectivity, access to cloud storage requires an internet connection.
- Organisations have only a limited amount of direct control over the physical infrastructure of cloud servers because server maintenance and security are handled by the cloud provider.
- When sensitive information is involved, the fact that cloud service providers have access to stored data might raise questions about ownership and privacy.

4. Threat model for a cloud-based streaming service

a) List of Assets

- Computational Resources
- Infrastructure such as servers
- Sensitive information
- Payment gateways
- Video files hosted in cloud
- User access

b) List of Entry points

- Sign in and Signup pages
- User management such as user profile and watch history
- Payment information
- Web interface

c) Attacker model:

Attacker capabilities

- basic understanding of vulnerabilities in online security.
- use of typical attack tools
- Should have the capacity to exploit security holes.
- Unauthorized access/Impersonation
- Data and password decryption

Attacker Motivation

- Theft of sensitive information
- Selling the data
- Demanding reward with victim

d) Vulnerabilities

- Attackers might pretend to be authorised users.
- unauthorised data access and modification to data
- sending a lot of requests at once to sabotage service.
- data collection during transmission.

e) mitigation strategies.

- Enable Two factor authentication
- Data minimization by limit the amount of private user data stored.
- secure communication connections and data storage.
- End to End encryption
- Train the workers of the service provider about security best practises.