**EXISTING SYSTEM**

The existing system for data leakage detection in cloud computing environment typically involves various tools and techniques aimed at identifying and preventing data breaches. These include:

1. Encryption: Data encryption is one of the most common methods used to protect data in the cloud. It involves encoding data in such a way that it becomes unreadable without a key.
2. Access Control: Access control mechanisms such as firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) are used to control who can access the data stored in the cloud.
3. Auditing: Regular auditing and monitoring of the cloud environment can help detect and prevent data leakage. It involves reviewing logs and other data sources for any suspicious activity.
4. Data Loss Prevention (DLP) Systems: These systems are designed to detect and prevent data leakage by monitoring data in transit and at rest.
5. Two-factor Authentication: This involves requiring users to provide two forms of authentication, such as a password and a security token, before they can access data in the cloud.
6. Virtual Private Network (VPN): VPNs can be used to provide a secure connection between the user's device and the cloud environment, preventing unauthorized access.

**DISADVANTAGES**

* **C**annot store the large volume of data and computational is less.
* Malicious data can attack the client file.
* Less accuracy and the performance is low.