|  |  |  |
| --- | --- | --- |
| Threats | Effects | Solutions |
| Different service delivery | Loss of control over the infrastructure of the cloud | provided services that were controlled and supervised |
| Misuse and criminal application of cloud computing | Due to unclear sign-ups, there is a loss of validation, service fraud, and a stronger attack. | Observe the state of the network and use strong registration, authentication methods. |
| Unsecured software interfaces and APIs: | Incorrect transfer of the content, improper, authentication, and authorization | Strong access control and authentication measures are used, and data transfer is secured. |
| Malicious insiders | resource penetration, asset damage, productivity loss, and operational impact | Utilization reporting and breach alerts, as well as open security and management procedures |
| Issues with shared technology in a multi-tenancy setting: | By exploiting the hypervisor, interfere with one user service and other user services. | Audit configuration and vulnerabilities, and utilise strong authentication and access control procedures for administrative tasks. |
| Data leakage and loss | Data that is personally sensitive may be altered, destroyed, damaged, or erased. | provide systems for data backup and storage |
| Service hijacking | Stolen user account credentials give access to a crucial region of the cloud, putting the security of the services at risk. | use of powerful authentication techniques, security guidelines, and encrypted communication |
| Risk profiling | Operations involving internal security, security guidelines, configuration breaches, patching, auditing, and logging | Recognize incomplete logs, infrastructure, and data aspects in order to safeguard the data use monitoring and altering system. |
| Identity theft | To access that user's resources and obtain credits or other benefits under that user name, an aggressor can obtain the identity of a legitimate user. | Authentication methods and strong multi-tier passwords should be used. |

Table 1: Different types of threats, their effects and solutions

**Attacks:**

|  |  |  |
| --- | --- | --- |
| Attacks | Effects | Solutions |
| Zombie attack | Affected service availability; possibility of creating a phoney service | robust authorisation and authentication |
| attack using service injection | Service integrity is compromised, and users are given malicious services in place of legitimate services. | Service integrity is compromised, and users are given malicious services in place of legitimate services. |
| port checking | Unusual service behaviour reduces service availability | Strong port security is necessary |
| Phishing attack | Affect the user's private information that shouldn't be shared | employ a secure web link (HTTPS) |
| attack through the backdoor | has an impact on the service's accessibility and data privacy, and offers rights for accessing legitimate user resources. | Strong authentication, identification, and isolation procedures are necessary. |