# Cloud Security Checklist

S.Venkatesan
Network Security and Cryptography Research Group
Indian Institute of Information Technology, Allahabad
venkat@iiita.ac.in

***End-User of the Cloud Service***

| Sl.No. | Attributes | Description |
|---|---|---|
| 1 | Strong Credentials | Not to use the weak or default credentials |
| 2 | Access from the Robust device | Ensure that the device from which the service is accessed is not having the keylogger, logs the activity, etc. |
| 3 | Use only Secure Connection | Always access through the HTTPS or SSH |

***Client Organization***

| Sl.No. | Attributes | Description |
|---|---|---|
| 1 | Identity and Access Management | Ensure the Access control of the services when there are more clients. |
| 2 | Activity Log | Record all the activities of the clients for the future auditing. |
| 3 | Hardening | Keep only the necessary software installed |
| 4 | Security Configuration | Implement Intrusion Detection/Prevention System, Firewall, etc. |
| 5 | Enable Security Features | By default enable all security features for the client. |
| 6 | Enforce Strong Credentials | The user should be forced to set the strong password. |

***Service Provider***

| Sl.No. | Attributes | Description |
|---|---|---|
| 1 | Secure Connection/Communication | Always the communication is through the secure channel TLS, IPSec, etc. |
| 2 | Enforce Strong Credentials | The user should be forced to set the strong password. |
| 3 | Secure Hypervisor – VM Hopping | Use the Secure Hypervisor to ensure the restriction of VM Hopping by the clients. |
| 4 | Client Isolation | No client should get the provision to see other |

| | | |
|---|---|---|
| | | client's data or process. |
| 5 | Secure VM image installation | Client can be allowed to install only the authentic VMs. |
| 6 | Access Control | Ensure the Access control of the services when there are more clients. |
| 7 | Secure Boot | TPM can be used to ensure the secure boot |
| 8 | Activity Log | Log all activities for the future auditing |
| 9 | Network Log | All communication log should be recorded for further analysis as and when required. |
| 10 | Encrypted Storage | Always store the data in the encrypted form. |
| 11 | Integrity | The data should not be modified and it should be identified if it is modified. Hashing algorithms and the TPM can be used. |
| 12 | Redundant Storage | Loss of data to the client organization is huge. The data should be stored in different locations for ensuring the availability. |
| 13 | Secure Remote Access | Always provide the secure access to client organizations. |
| 14 | Enable Security Features | By default enable all security features for the client. |
| 15 | Enforce Strong Credentials | The user should be forced to set the strong password. |
| 16 | Control Access of Client Data by Provider | Administrator should not get provision to access the client data without their knowledge. |