**IoT Liability**

IoT is Internet of thing as the term itself says it is connecting things to internet. As a connecting medium for networking is an IP and port. Any device or thing, which has identity in-terms of IP and ports are prone to security attacks

Any secured platform may have means to attack; containing the attack not allowing spreading wild will be first defensive mechanism in security attack.

Rotating access token and certificates from firmware using OTA and changing device data sampling rate may solve the brute force attack. Simple setting of rules with respect to data rate if data rate set is not matching the data rate received a suspicious activity is detected.

As IoT devices are exposed to air and sometimes it is accessible to thieves. So proper casing depending upon on deployment and protecting it from some casing from tampering and theft.

Deployment of IoT solution should make the product customer friendly and liable. The IoT device deployed should be free from hang and should provide a mechanism to operate the device in case of network failure or Internet issues.

User should be free to use solution deployed based on his choice. User should not be forced to use IoT apps or webapps forefully.

Though connecting things gives powerful integration and productivity, they also create perfect opportunity for cyber-attacks like hacked stove or fire safety sprinkler system.

The best measures against cyber-attack addressed through providing custom protections such as monitoring and access privileges and providing hierarchal architecture.

Cyber-attack consists of simple measures like

* **Built-in Security**
* **Encryption**
* **Risk Analysis**
* **Authorization**