**IoT Security**

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. From the application security, CA signed certificates for browsers handle it. Protocol level, MQTT has encryption using 8883 port and CoAP has DLS as part of datagram.

Device provisioning should be taken as top priority task by using access token for normal applications and X.509 certificates for critical applications.

IoT platforms has proper access for users in terms of username and passwords. Some platforms also has hierarchical approach in terms of tenant, customer and user relationship restricting access to platform for different roles.

The device and platforms is linked through certificate or access token have to be rotated periodically to prevent platform from attack.

If devices which are unable to communicate in terms of standard IoT protocols like MQTT , CoAP and HTTP (ie.,access token or certificates) and the only way they communicate is TCP/UDP or legacy protocol. These devices are prone to masquerader attack. So, to prevent these type of attack these devices communicate to IoT gateways and IoT gateways encrypts their data and send to platform. Any attacks happens is now restricted to gateway and platform can stop data streamed from gateway by just blocking the port. Thus, IoT gateways plays an important role in containing the attack.

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.

In conclusion, connecting things has an advantage but is security is not properly handled it may lead to catastrophic damages like connected cars controlled by hacker and smart home controlled by hacker are to name few.