**IoT identity protection**

IoT platforms are cloud-based servers, which runs 24x7 against applications that run on-premises locally. Server-based solutions, which runs locally, will have to maintain by human resource and scaling will be an issue. These issues are resolved easily in cloud-hosted solution and the user can pay as per usage. IoT with the cloud-based solution will be a part of the server side. The client side can be from a tiny microcontroller to computers.

The data expected in IoT is strings or strings like JSON and with maximum rate of transfer. i.e., 1000 messages per second. To handle this type of data type, IoT uses dedicated lightweight protocols like MQTT, CoAP, and HTTP depending on use cases. Study says with the advent of IoT protocol MQTT (Message queuing telemetry transport) 70% of data is collected as against to 20% before MQTT. MQTT is application layer; publish/subscribe architecture-based protocol built on top of Transport control protocol (TCP). MQTT has three quality of services in addition to TCP, which is connection oriented and reliable transport control protocol. Broker is heart of the architecture, which facilitates exchange of information between publishers and subscribers. Publishers are data generators, subscribers are data consumers, and they connected via broker. Publishers and subscribers are just clients to the broker. Broker is responsible for authentication of client and maintain the subscription list of topics.

MQTT protocol is comparable to YouTube. YouTube has many channels and user is be subscribed to channel of their interest. If an upload done on subscribed channel, the entire subscribers gets the alert. Therefore, users get the alert for only channels for which they have subscribed for and not for other channels as YouTube is running many channels.

Another example is Facebook post; any post done by user will act as publisher and friends on user acts as subscribers. When a Facebook post posted all the friends of the particular account gets the post.

For an example, Thingsboard on IoT platform uses access token or X.509 certificates

The embedded device is physical entity and the logical entity is created in platform that is popularly knowns as device provisioning.

The data sent from physical devices has to be uniquely identified as a logical entity in platform. Physical devices are uniquely identify username, passwords, Access tokens and certificates, which identifies the physical devices logically.

This is how identity of logical device is identified in IoT platform. If this access token and certificate is compromised, anybody will be able to send data. So, there should be way to address this issue by rotating certificates or access token.