Authentication, Authorization of devices:

Authentication and authorization are two crucial components in the ongoing effort to keep Internet clients and devices safe. Because, at its most basic level, the Internet of Things is just devices—from simple sensors to complicated automobiles and mobile devices—connecting together to share data, these components are critical to any IoT project. These connections need to be protected, and authentication and authorization can help.

Authentication- The process of recognizing the device is known as authentication. The authentication method for Message Queuing Telemetry Transport (MQTT) is to ensure that the device's client ID is valid, that is, that the ID belongs to the device in question.

Authorization- It is a method of associating a certain device with specific permissions. Authorization is split into two steps using Edge Connect:

- Associating devices with groups
- Creating a link between groups and issues

Authentication
The process of recognizing the device is known as authentication. The
authentication method for Message Queuing Telemetry Transport (MQTT) is
to ensure that the device's client ID is valid, that is, that the ID belongs to the device in question.

Device based authentication and authorization :

Device-based authentication and authorization will most likely be utilized for devices that do not have operators (or users), or for devices where the connection is not dependent on the operator.

An automobile is an excellent example: whether or not the car has user-specific communication—such as running user applications or offering user-specific

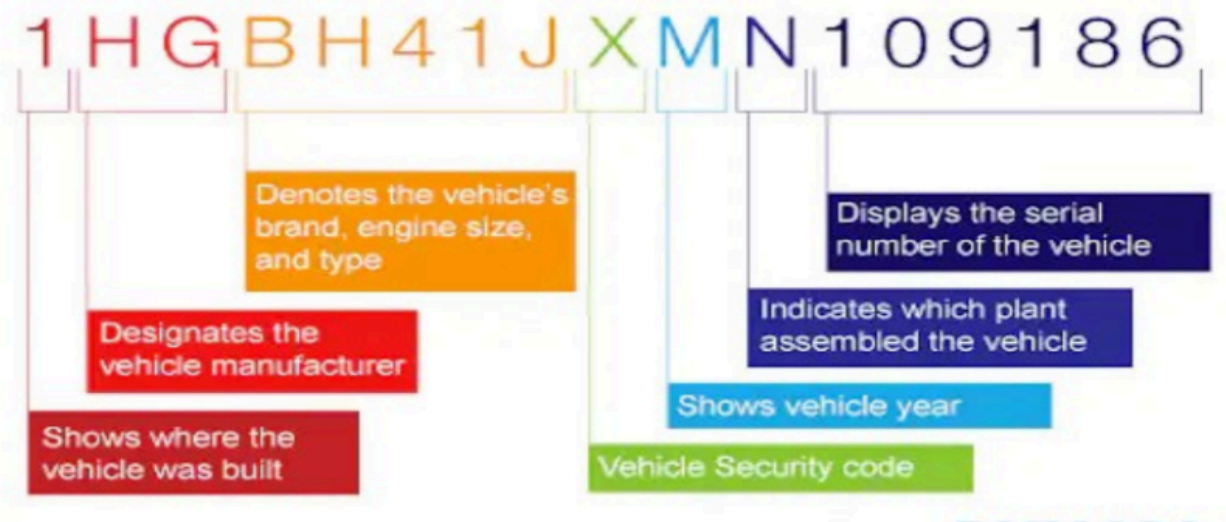
configurations—the device (i.e., the car) will most likely wish to be linked to share car-specific information.

Diagnostics, command and control, software updates, and advanced feature availability are all examples of data that is exclusive to the car rather than the driver.

After the car has been validated and the client ID has been determined, the proper authorization groups must be determined. A device can join an authorization group simply by connecting. Because the device in this case is a car, all automobiles that connect will be assigned to the authorization group "car." Additional groups, just like the client ID, can be derived from the certificate. The VIN of our car, for example, can be used to extract a range of groups . However, the certificate/VIN can also be used to derive the brand and year.

User - based authentication and authorization:

The person is the focus of user-based authentication and authorization rather than the device. While a device must still offer a unique device ID, the authorization groups in this case are determined by the user's identification.



ACCESS CONTROL:

Three FCs(functional components) in a security FG(function group) for ensuring security and privacy are: ● Authentications

● Authorisation

● Key exchange and management

Authentication: ID establishment and authentication are essential elements of access control. A hash function or MD5 gives the irreversible result after many operations on that and the operations are just one way. The algorithm generates a fixed size, say, 128 or 256-bit hash or digest value using authentication data and secret key. Only the hash or digest value communicates.

Authorization: Access control allows only an authorised device or application/service access to a resource, such as web API input, IoT device, sensor or actuator data or URL. Authorisation model is an essential element of secure access control.

The standard authorization models are as follows:

● Access Control List (ACL) for coarse-grain access control

● Role-Based Access Control (RBAC) for fine-grain access control

● Attribute-Based Access Control (ABAC) or other capability-based fine grain access control

Structured vs unstructured data:

Characteristic	**Structured Data**	**Unstructured data**
Nature of data	Usually quantitative	Usually qualitative
Data model	Pre-defined; once it is defined and some data stored, it is difficult to change the model	No particular schema is involved in unstructured data; the data model is very flexible
Data format	A limited number of data formats are available	A huge variety of data formats are available for unstructured data
Database	SQL-based relational databases are used	No SQL databases with no specific schema are used

Search	Very easy to search and find data within the database or data set	Very difficult to search for particular data due to its unstructured nature
Analysis	Very easy to analyze, given the quantitative nature of data	Very difficult to analyze, even with existing software tools
Storage method	Data warehouses are used for structured data	Data lakes are used to store unstructured data

UNSTRUCTURED DATA STORAGE ON CLOUD/LOCAL SERVER

Different methods of data collection, storage and computing are shown in below Figure. It shows:

(i) Devices or sensor networks data collection at the device web server,
(ii) Local files,
(iii) Dedicated data store at coordinating node, Local node in a distributed DBMS,
(iv) Internet-connected data centre,
(v) Internet-connected server,
(vi) Internet-connected distributed DBMS nodes, and
(vii) Cloud infrastructure and services.

Cloud computing paradigm is a great evolution in Information and Communications Technology (ICT). The new paradigm uses XAAS at the Internet connected clouds for collection, storage and computing.

XaaS stands for "Anything as a Service" or "Everything as a Service" and is a cloud computing concept that allows users to access a variety of services, applications, and resources over the internet.