Welcome students, this program is for the Bachelor of Science third year students for the subject of computer science which is for the Semester 6 having the course code as CSC110 and Course title as Internet of Things.

Next, this is for Unit 1 for IoT concepts having the module name as connectivity protocols which comprises of MQTT and SMQTT.

So the basic outline for this module is we will be studying about MQTT, then MQTT architecture and its component, broker based MQTT protocol and SMQTT.

So the students will be able to learn the MQTT architectures, the different protocols and its components. They will also learn about SMQTT.

So first we'll study about the MQTT. So MQTT stands for Message Queue Telemetry Transport. So it is basically a lightweight message queuing and transport protocol which is designed to provide connectivity mostly through embedded systems between the applications and middle-ware. A message broker controls the publish-subscribe messaging pattern. So MQTT is basically designed for remote connections, limited bandwidth applications, and some small code footprints.

So this is the basic architecture of the MQTT, which comprises of publishers and subscribers, and we have an endpoint that is the broker queue or topic endpoint which is at the middle.So we'll see about each one of them.

So the MQTT architecture components comprises of, first is the publisher. So publishers are nothing but the lightweight sensors that connect to the broker to send their data and go back to sleep whenever it is possible. Next we have the subscribers, which are nothing but the applications that are interested in certain topic or some sensory data so they can connect to the broker to be informed whenever new data is received. And finally we have the brokers which classifies the sensory data into topics and then send them to the subscribers which are interested in that topics.

Next are the MQTT methods. So MQTT methods can consist of connect, which opens a new connection to the MQTT broker. Then have disconnect, which can close that open connection to an MQTT broker. Next we have something called as subscribe method, which subscribes to one or more specific MQTT topics. Then we have unsubscribe, which will stop subscribing to one or more MQTT topics, And finally we have the publish. So publish at MQTT client can publish this message is as soon as is it connects to a broker.

So this is basically the protocol architecture for a broker based MQTT which comprises of the publisher, broker and subscriber having the different components that is connect, connect- acknowledgement and publish and subscribe.

So here MQTT protocol architecture uses a publish- subscribe architecture that is, the HTTP using a request-response paradigm. So publish or subscribe is an event driven and enables the messages to be

pushed to the clients. The central communication point that is the MQTT broker which is in the charge of dispatching all the messages between the senders and the rightful receivers. So each client that publishes this message to the broker includes a topic into the message. Now this topic is nothing but is the routing information which is sent to the broker.

So each client that wants to receive this messages subscribes to a certain topic and the broker which delivers all these messages with the matching point to the client. Therefore, the client doesn't have to know each other, they only communicate over the topic. So this architecture basically enables highly scalable solutions without the dependencies between their data producers and data consumers.

Next is something called as SMQTT. So it is basically an extension to the simple MQTT protocol. So SMQTT stands for Secure Message queue telemetry transport. It is also uses lightweight attribute based on your encryption. So it is a session layer protocol.It has a broadcast encryption feature which does encryption of one message and delivers the same to multiple nodes. So the algorithm for SMQTT is divided into four parts that are your setup, encryption, publish and decryption. So like MQTT it uses your broker based subscribe and publish architecture.

Next, we'll see what are the different phases of this algorithm. So the first phase is your setup phase. Here the subscribers and the Publishers register themselves with the broker, and they obtain a master secret key for it. The second phase is the encryption. So in encryption the data is being encrypted. Next we have the publish phase. Here the encrypted data is published by the broker and this is being then received by the subscriber. The last phase is the decryption phase, which performs the decryption of two decode of the data with the same master. So your key generation algorithm is not standardized over here, and it depends on the developers. Encryption algorithm depends on the developers too.

So these are my references for this course. Thank you.