Project Design Phase-II
Solution Requirements (Functional & Non-functional)

Date	03 October 2022
Team ID	PNT2022TMID11911
Project Name	IOT Based Smart Crop Protection System for Agriculture
Maximum Marks	4 Marks

Functional Requirements:

FR No.	Functional Requirement (Epic)	Sub Requirement (Story / Sub-Task)
FR-1	Resource discovery	The specifications define the common services provided by the application service layer in IOT systems, referred to as common service functions. 'Discovery' is one of the defined CSFs which allow IOT entities to send discovery requests to search resources about applications and services.
FR-2	Resource management	The resources considered in Table 1 include battery-time, memory usage, and other data related to application performance to make quality of service reliable. Although some parts of this requirement rely on its implementation of the 'Application and Service Layer Management' and 'Device Management' could probably support these requirements.
FR-3	Data management	The 'Data Management and Repository' is responsible for providing data storage and management converting aggregated data into a specific format and preparing for further analytics such as semantic processing.
FR-4	Event management	The 'Subscription and Notification' can manage subscription to the resources hosted in the platform, and can provide notification containing the changes on the resources to the address where the subscriber wants to receive them. Accordingly, application and services can acquire all the information about the proper events in real-time.
FR-5	Code management	The 'Device Management' utilizes the already-existing technologies including broadband forum (BBF) TR-069, OMA-DM, LwM2M for managing device capabilities. Of course, code updating operations for IOT devices could be achieved with the help of management clients, servers, and adapters specifications.

Non-functional Requirement:

FR No.	Non-Functional Requirement	Description
NFR-1	**Usability**	The 'Device Management' allows the application entities registered to a server platform to be easily maintained through existing device management technologies. Also, the Node.js-based implementation enables the middleware components to be updated or replaced accordingly without any high-level of technical expertise.
NFR-2	**Security**	Security is a very critical requirement in IOT solutions and defines its security framework including identification, authorization and authentication. Our middleware platform can be registered to the server (i.e., Mobius) as an application entity. It can attempt to access a list of authorized resources hosted by the server with its server-generated unique identifier and privileges, called access control policy. However, authentication and other security components such as certificates still remain incomplete.
NFR-3	**Reliability**	we have not yet realized capabilities related to Reliability, which allows platform-equipped devices to adapt themselves according to short-term or long-term changes in resource conditions, application scenarios, and surrounding environments, remaining our future work.
NFR-4	**Performance**	This requirement belongs to a part of intelligence for IOT devices, and the proposed IOT device platform provides no analytic tools on data or decision-making procedures depending on resource conditions, for example, recommending the most suitable (or currently available) one among multiple IOT devices offering the same service, which is one area of our future work.
NFR-5	**Availability**	Availability could be achieved by ensuring some level of fault-tolerance. The developed IOT platform does not deal with all fault tolerance issues that mainly occur in hardware interfaces. However, a watchdog function is able to detect the failure of middleware components interacting with hardware interfaces, and restart or reconnect if needed.
NFR-6	**Scalability**	An IOT platform needs to support rapidly growing numbers of IOT devices and keep a certain level of support. Although the scalability of an IOT platform is crucial, it highly depends on implementation and performance in IOT servers rather than connected devices. Accordingly, in support of a well-designed - based IOT server we can say that our middleware platform may deliver some level of appropriate for the given environment and applications.