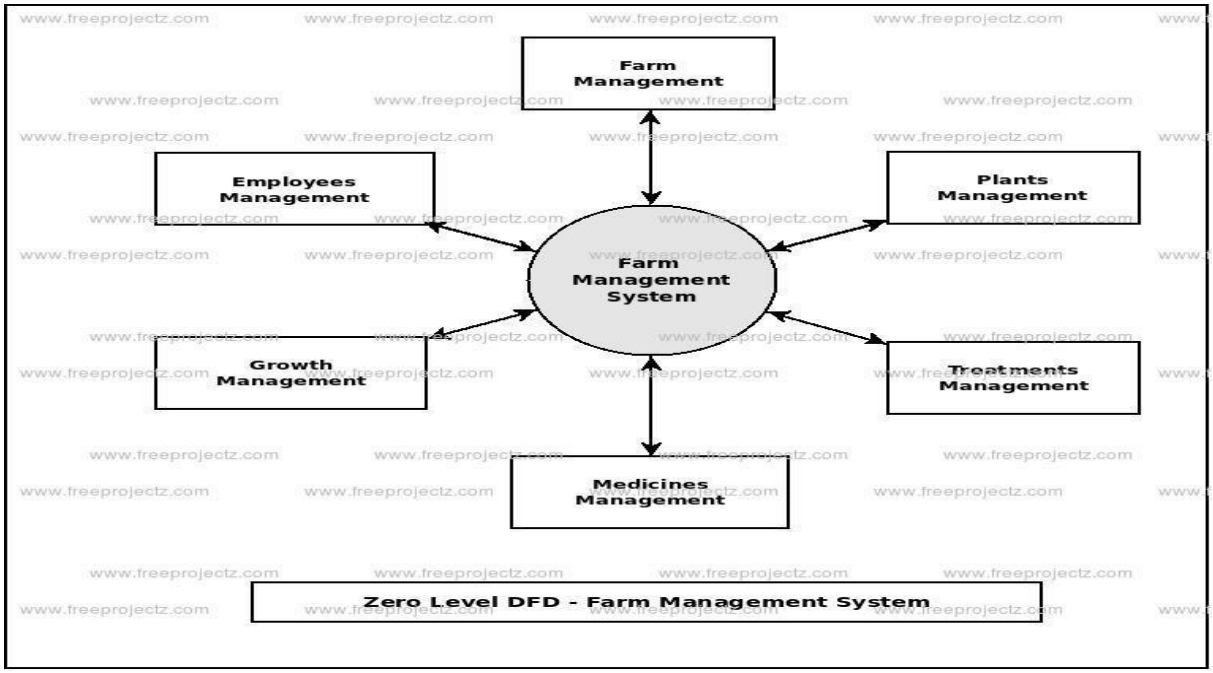
Project Design Phase – II

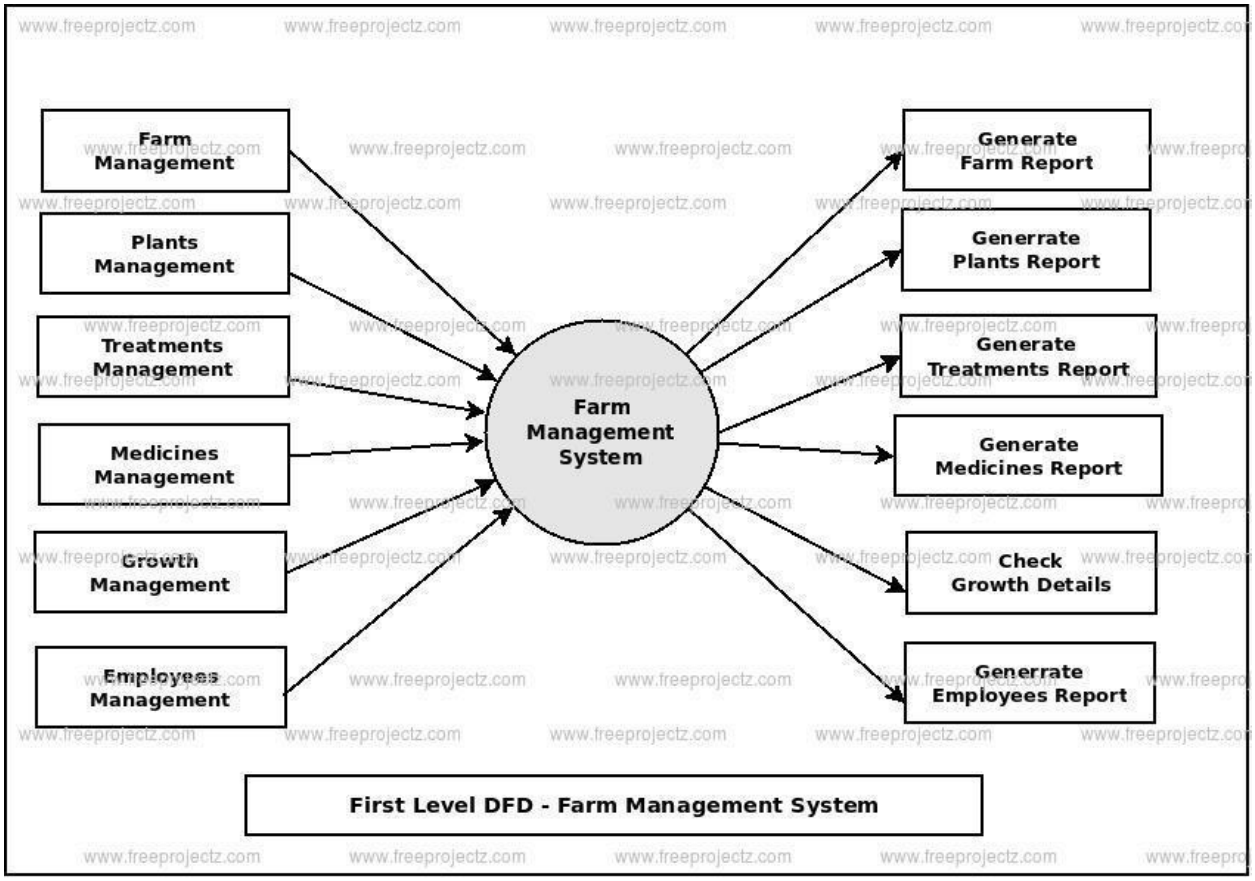
Data Flow Diagram & User Stories

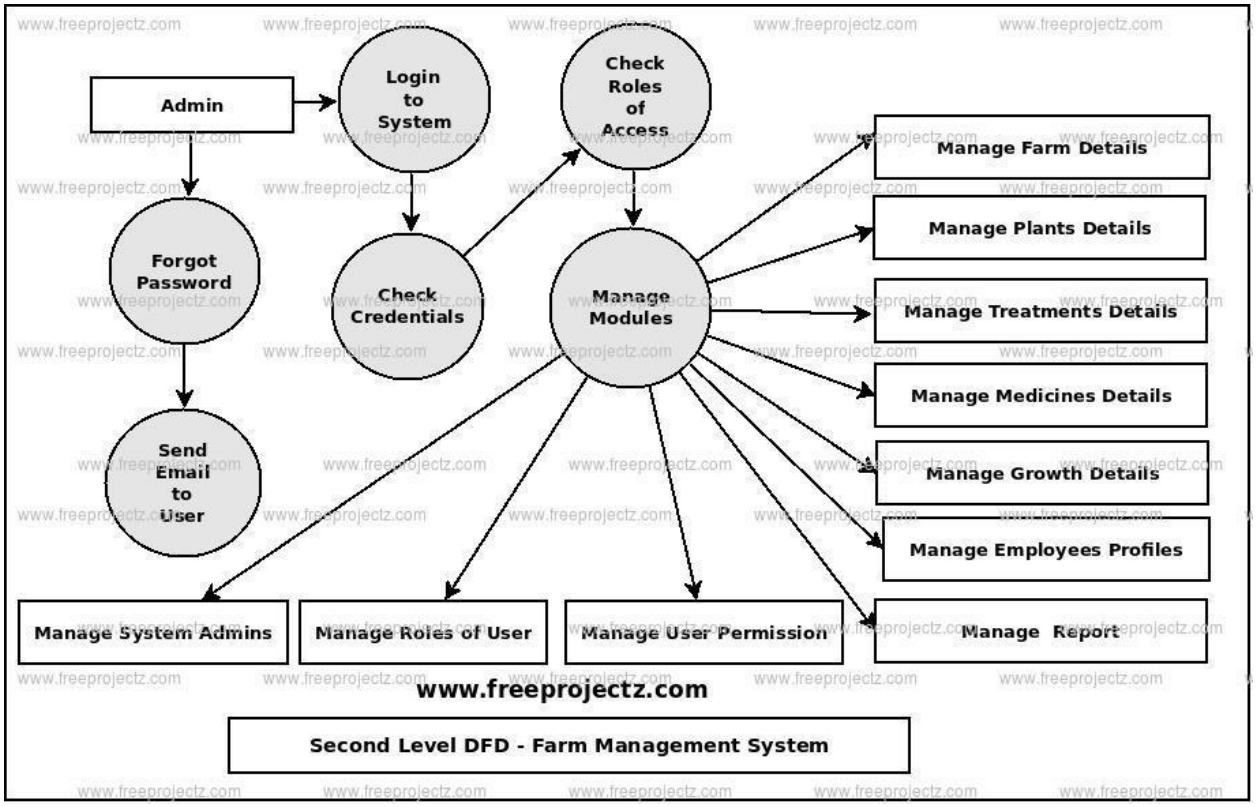
Team id	PNT2022TMID41344
Project name	Smart farmer – iot enabled smart farming application

Data Flow Diagrams:

A Data Flow Diagram (DFD) is a traditional visual representation of the information flows within a system. A neat and clear DFDcan depict the right amount of the system requirement graphically. It shows how data enters and leaves the system, what changes the information, and where data is stored.




Farm Management
Plants Management
Treatments Management
Medicines Management
Growth Management
Employees Management
Farm Management System
Generate Farm Report
Generrate Plants Report
Generate Treatments Report
Generate Medicines Report
Check Growth Details
Generrate Employees Report
First Level DFD - Farm Management System



There are certain challenges you need to be aware of if you are considering investing into smart farming.

1. The hardware

To build an IoT solution for agriculture, you need to choose the sensors for your device (or create a custom one). Your choice will depend on the types of information you want to collect and the purpose of your solution in general.

In any case, the quality of your sensors is crucial to the success of your product: it will depend on the accuracy of the collected data and its reliability.

2. The brain

Data analytics should be at the core of every smart agriculture solution. The collected data itself will be of little help if you cannot make sense of it.

Thus, you need to have powerful data analytics capabilities and apply predictive algorithms and machine learning in order to obtain actionable insights based on the collected data.

3. The maintenance

Maintenance of your hardware is a challenge that is of primary importance for IoT products in agriculture, as the sensors are typically used in the field and can be easily damaged.

Thus, you need to make sure your hardware is durable and easy to maintain. Otherwise you will need to replace your sensors more often than you would like.

4. The mobility

Smart farming applications should be tailored for use in the field. A business owner or farm manager should be able to access the information on site or remotely via a smartphone or desktop computer.

Plus, each connected device should be autonomous and have enough wireless range to communicate with the other devices and send data to the central server.

5. The infrastructure

To ensure that your smart farming application performs well (and to make sure it can handle the data load), you need a solid internal infrastructure.

Furthermore, your internal systems have to be secure. Failing to properly secure your system only increases the likeliness of someone breaking into it, stealing your data or even taking control of your autonomous tractors.

6. Connectivity

The need to transmit data between many agricultural facilities still poses a challenge for the adoption of smart farming. Needless to say, the connection between these facilities should be reliable enough to withstand bad weather conditions and to ensure non-disruptive operations.

Today, IoT devices still use varying connection protocols, although the efforts to develop unified standards in this area are currently underway. The advent of 5G

and technologies like space-based Internet will, hopefully, help find a solution to this problem.

7. Data collection frequency

Because of the high variety of data types in the agricultural industry, ensuring the optimal data collection frequency can be problematic. The data from field-based, aerial and environmental sensors, apps, machinery, and equipment, as well as processed analytical data, can be a subject of restriction and regulations.

Today, the safe and timely delivery, and sharing of this data is one of the current smart farming challenges.

8. Data security in the agriculture industry

Precision agriculture and IoT technology imply working with large sets of data, which increases the number of potential security loopholes that perpetrators can use for data theft and hacking attacks. Unfortunately, data security in agriculture is still, to a large extent, an unfamiliar concept.

Many farms, for example, use drones that transmit data to farm machinery. This machinery connects to the Internet but has little to zero security protection, such as user passwords or remote access authentications.

Some of the basic IoT security recommendations include monitoring data traffic, using encryption methods to protect sensitive data, leveraging AI-based security tools to detect traces of suspicious activity in real-time, and storing data in the blockchain to ensure its integrity.

To fully benefit from IoT, farmers will have to get familiar with the data security concept, set up internal security policies, and adhere to them.