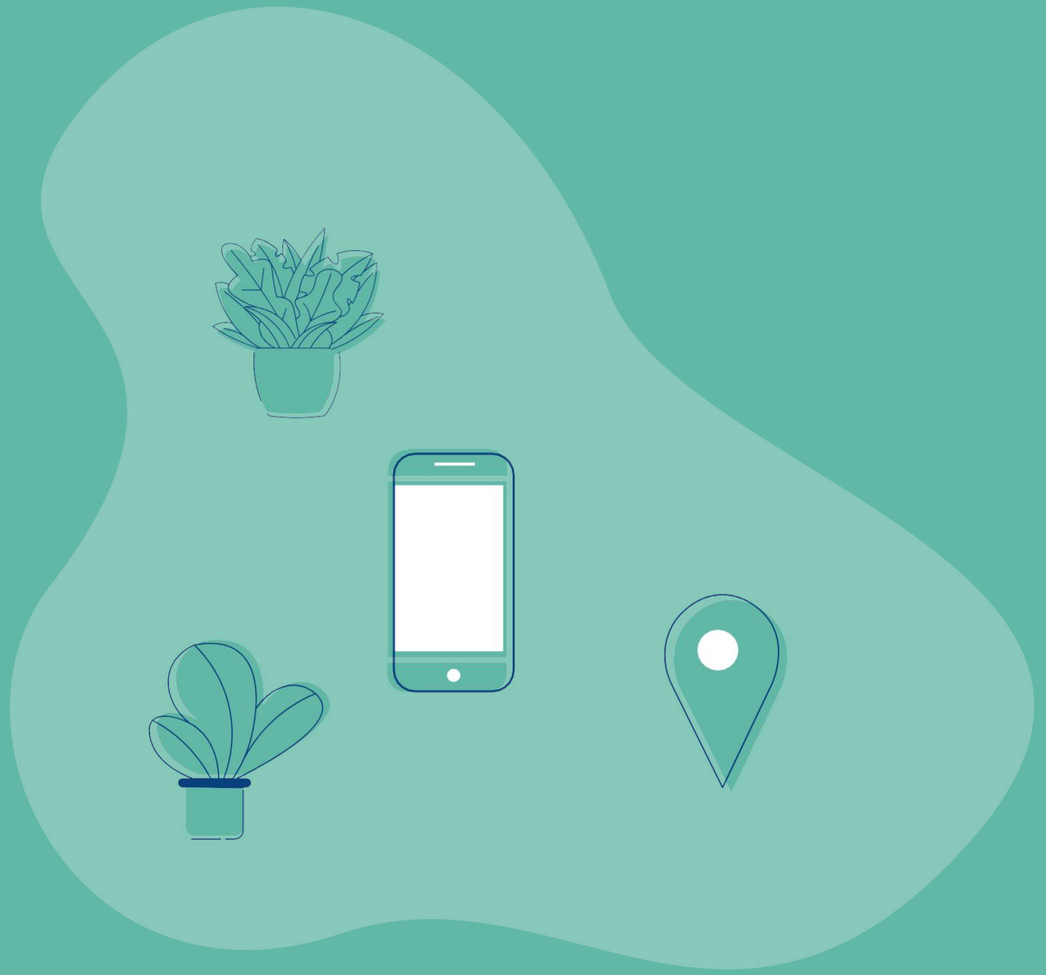
Smart Farming Using IOT.

Cyber threats and attacks in smart farming.

Deepak C Varghese



Internet of Things

The Internet of things refers to a type of network to connect anything with the Internet based on stipulated protocols through information sensing equipments to conduct information exchange and communications in order to achieve smart recognitions, positioning, tracing, monitoring, and administration.

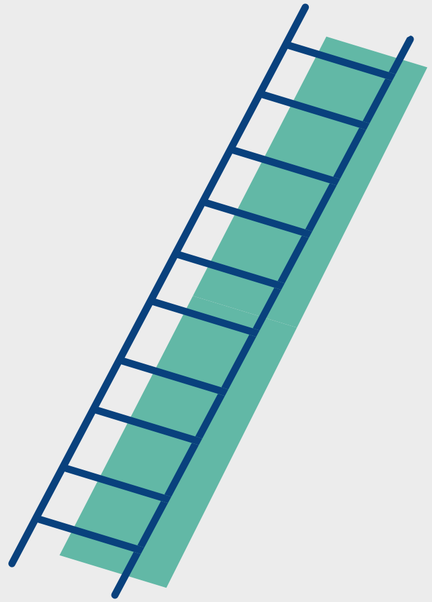
Scope

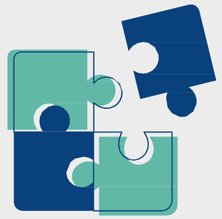
According to the World Health Organization, 420,000 people die every year from food-related illnesses and 600 million people fall ill as a result of food contaminated with bacteria, viruses, toxins or chemicals. A cyber attack on the food ecosystem targeted at farms, transportation system, or food processing industrial control systems may increase these numbers exponentially.

Identifying the vulnerability

Analysing the problem

Inclusion of prevention measures





Types of threats:

1. **Physical threats**

   It can happen if the system is damaged physically due to natural disasters. (Hacker can intrude into a network if the firewall server is down)

2. **Accidental errors**

   Exceptions which were not handled in the architecture while designing. (Hackers can misuse the loopholes in design to get inside the system and deploy malicious softwares)

3. **Unauthorized access**

   Accessing a system which is above the privileges without proper permission.

4. **Malicious misuse.**

   Tampering of the system which includes penetration, Trojan horse, viruses.

Most common threats:

1

Denial of Service

Attacks not only can disrupt normal functions of different modules in anindividual farm but also can be leveraged to interrupt legitimate cyber services in other domains.

2

Data attack

Insider data leakage, cloud data leakage, false data injection(Compliance and Regulation policies can be affected based on the false data injected),misconfigurations

3

Network attack

Frequency jamming of WiFi or GPSsystem

4

Other relevant atacks

cyber terrorism(agro-terrorism)

Causes:

Human error

Errors occurring in human perspective

Computer Abuse or crime

Cyber attack or threat

Natural disaster

System damage which occurs due to natural disaster

Hardware or software failure

For example if a Hardware firewall server fails, then the entire system is vulnerable.

What a hacker can do:

Read

Read unauthorized files.

write

Change or modify existing data in the system.

Delete

Delete confidential data or packages resulting in business loss

Create and Execute

Create and execute malicious code in the systems.

Solutions:

1

Data encryption

Data transfer and communication between the devices and the users over the network can be encrypted.

2

Strong authentication

We can use a strong authentication in the network for users as well as connection requests from individual devices in IoT

3

Closing unused ports

Unused ports can be kept closed to avoid any illegal entry to the system

Solutions:

4

Auditing

All the objects connected to the IoT network should be monitored and logs should be analysed to detecr any security threats.

5

Intrution Detection System

IDS system can be used with proper alert system and business analytics to monitor the intrutions

6

MAC/IP filtering

We can provide system access to the authentic devices only by ffiltering their device ID.

7

Software updates

All the softwares and firmware should be updated. Devices with vulnerabilities should be avoided.

Any Questions ?