A review of the different types of attacks at different layers of an IoT-enabled Skin Monitoring System

- ⇨ For IOT it consists of 3 major layers:
  - ⇨ Perception Layer
  - ⇨ Network Layer
  - ⇨ Application Layer

Perception Layer: It is the upper and physical layer of architecture, in this we have sensors for sensing and all and it consist of sensors like RFID barcodes or any other sensor. In this sensors identifies and collect the information.

Some of the attacks in perception layer are like in this we have Smart Card, RFID tags, etc.. and in this we knows that in RFID implementation it provides unique identification of the objects that are attached to that code or tag and in this the most common attacks can be like:

- ⇨ Unauthorized tag disabling
- ⇨ Unauthorized tag cloning
- ⇨ Unauthorized tag tracking

Some more physical attacks can be:

- ⇨ Brute Force attack: Resource storage, computation of the sensors will suffer more in that category.
- ⇨ Routing attack: In this like data forwarding, intermediate nodes can attack the data during forwarding.
- ⇨ Dos attack: Nodes can easily be trapped under DoS attack, given their finite processing ability.
- ⇨ Node Privacy Leak: The attackers can steal sensitive information in the node.
- ⇨ Spoofing: When an attacker broadcasts fake information to the RFID Systems and makes it assume its originality which makes it appearing from the original source.

Network Layer: In this we send the data (which we collected from perception layer) to network devices like servers, wifi, different IOT hubs etc…

Some kinds of attacks in network layer are:

- ⇨ Hello Flood Attack: It causes high traffic in channels by congesting the channel with a number of useless messages.
- ⇨ Selective Forwarding: In this a node sends few selective nodes instead of all the nodes.
- ⇨ Acknowledgement Flooding Attack: In this a malicious node sends false information to the neighbouring nodes.
- ⇨ Sleep Deprivation Attack: It is the kind of attack which keeps the nodes awake resulting in more battery consumption and as a result battery lifetime is minimized which causes the nodes to shut down.
- ⇨ Malicious Code Injection Attack: In this attacker compromises a node to inject malicious code into the system which could even result in a complete shutdown of the network.

Application Layer: In this we have IOT based applications, in this we store the data process it and remain confidential. In this

Attacks on application layer are:

- ⇨ Privacy Leak: In this the application of IoT is executed on common operating systems and the attacker can easily steal user data by known vulnerabilities.
- ⇨ Malicious Code Injection: In this attacker leverage the attack on the system from end-user with some hacking techniques that allows the attacker to inject any kind of malicious code into the system to steal some kind of data from the user.
- ⇨ Phishing Attack: In this user or victim is lured into opening the email through which the adversary gains access to the credentials of that victim and then by retrieves more sensitive information.
- ⇨ Sniffing Attack: In this attacker can force an attack on the system by introducing a sniffer application into the system, which could gain network information resulting in corruption of the system.

***** THANK YOU*****