



SNS COLLEGE OF ENGINEERING

Kurumbapalayam(Po), Coimbatore – 641 107

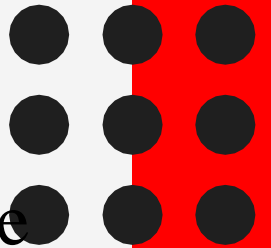
An Autonomous Institution

Accredited by NAAC-UGC with 'A' Grade

Approved by AICTE, Recognized by UGC & Affiliated to Anna University, Chennai

UNIT 1

IOT FUNDAMENTALS



IOT FUNCTIONAL BLOCKS

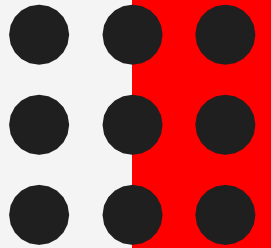
IoT security refers to the methods of protection used to secure internet-connected or network-based devices. The term IoT is incredibly broad, and with the technology continuing to evolve, the term has only become broader. From watches to thermostats to video game consoles, nearly every technological device has the ability to interact with the internet, or other devices, in some capacity

1. Remote exposure

Unlike other technologies, IoT devices have a particularly large attack surface due to their internet-supported connectivity. While this accessibility is extremely valuable, it also grants hackers the opportunity to interact with devices remotely. This is why hacking campaigns like phishing are particularly effective. IoT security, like cloud security, has to account for a large number of entry points in order to protect assets.

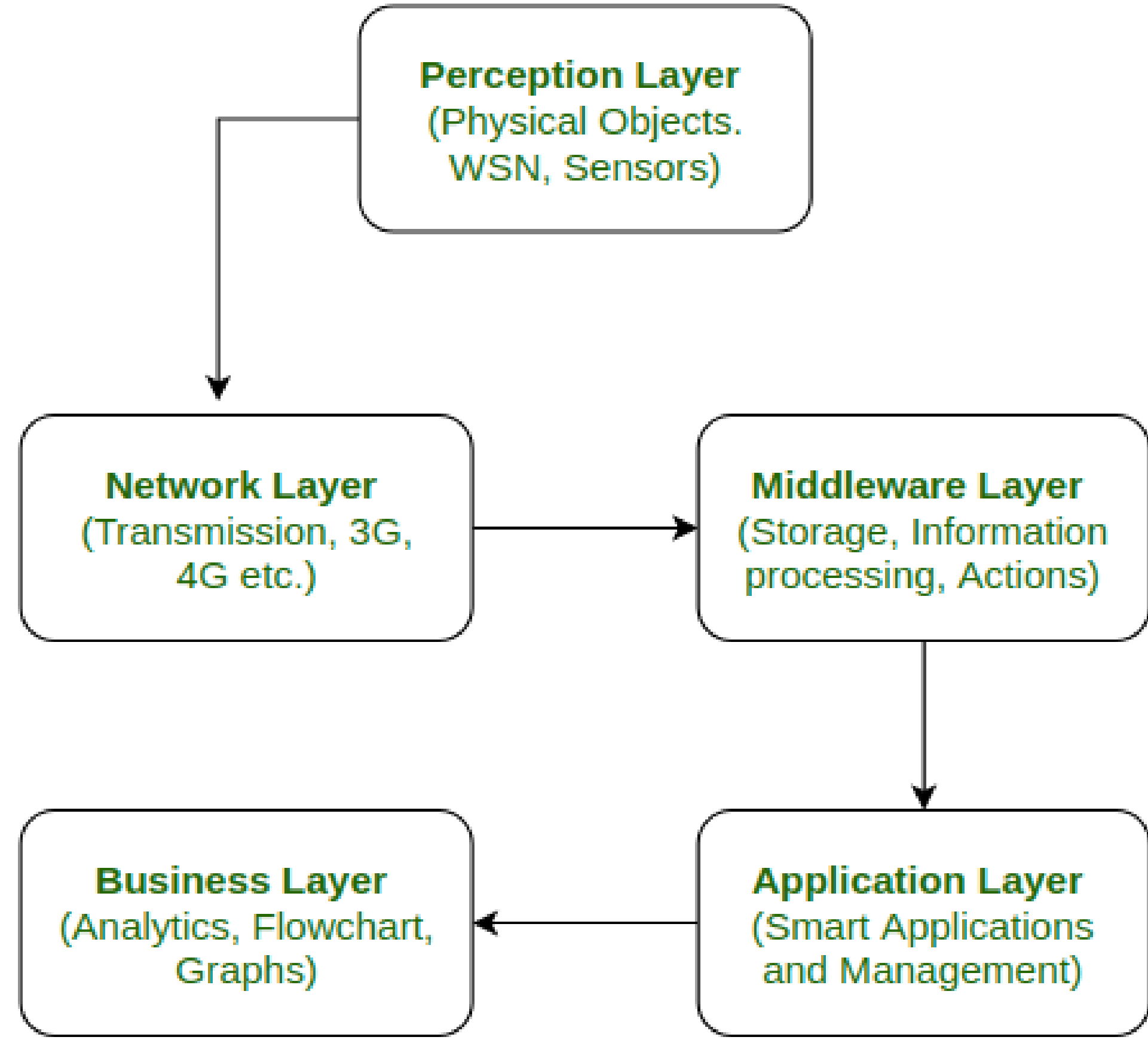
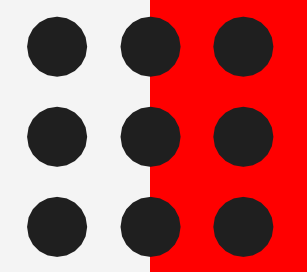
2. Lack of industry foresight

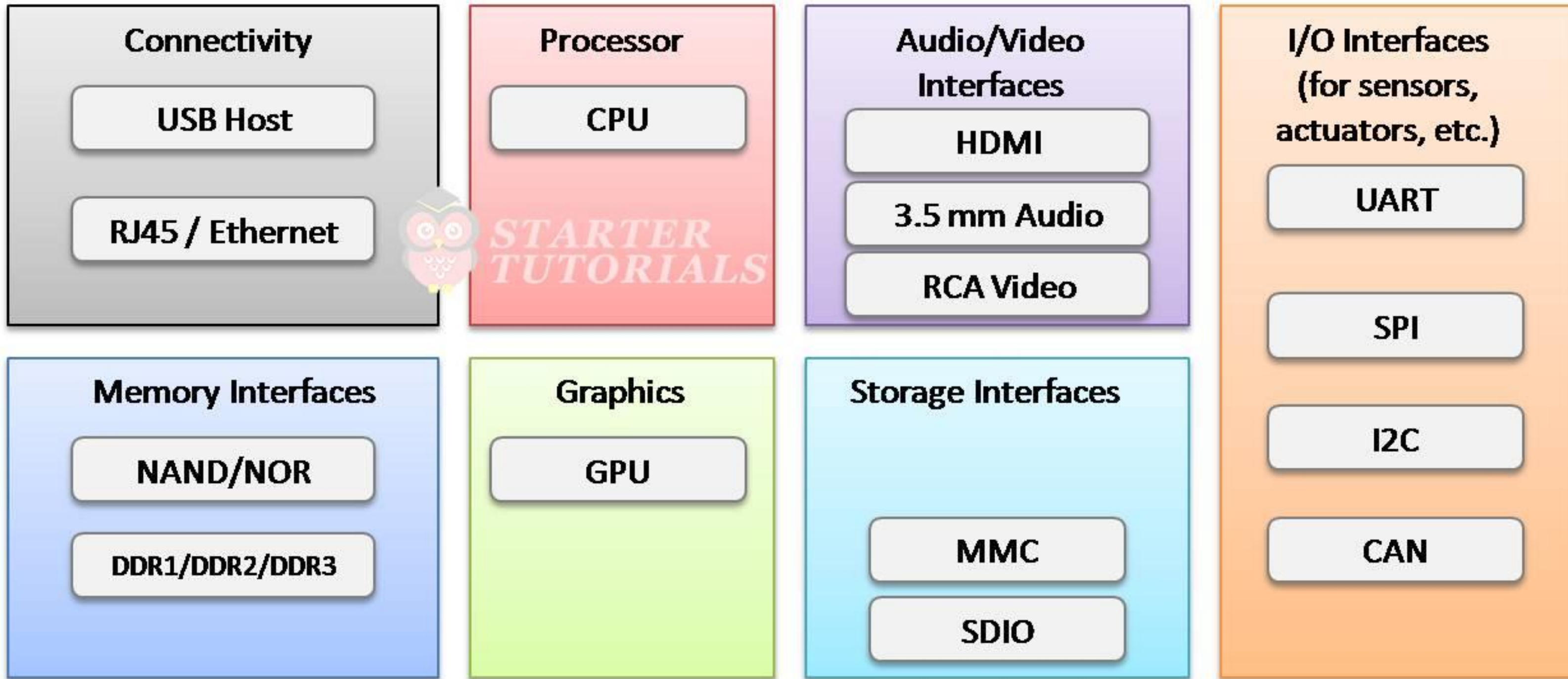
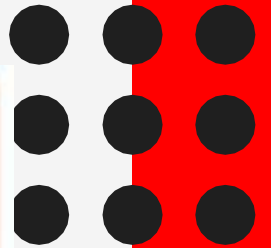
As firms continue with digital transformations of their business, so, too, have certain industries and their products. Industries such as automotive and healthcare have recently expanded their selection of IoT devices to become more productive and cost-efficient. This digital revolution, however, has also resulted in a greater technological dependence than ever before.

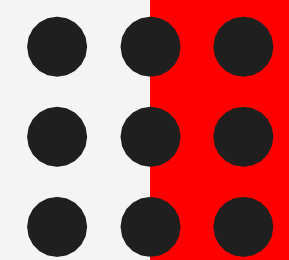
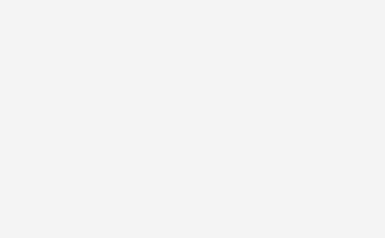


3. Resource constraints

Lack of foresight isn't the only IoT security issue faced by newly digitized industries. Another major concern with the IoT security is the resource constraints of many of these devices. Not all IoT devices have the computing power to integrate sophisticated firewalls or antivirus software. Some barely have the ability to connect to other devices. IoT devices that have adopted Bluetooth technology, for example, have suffered from a recent wave of data breaches. The automotive industry, once again, has been one of the markets hurt the most.







THANK YOU