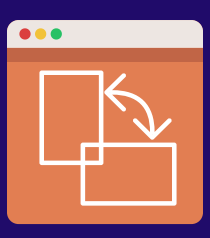
Vulnerabilities Of IoT

Internet of Things (IoT) offers extensive connectivity of devices for facilitating user convenience. However, it is important to pay attention to IoT vulnerabilities for cyber security.

Hackers can gain access to connected devices through vulnerabilities such as unsecured network (arising due to open ports like UPnP, UDP) or exploitable services such as buffer overflow & DoS.

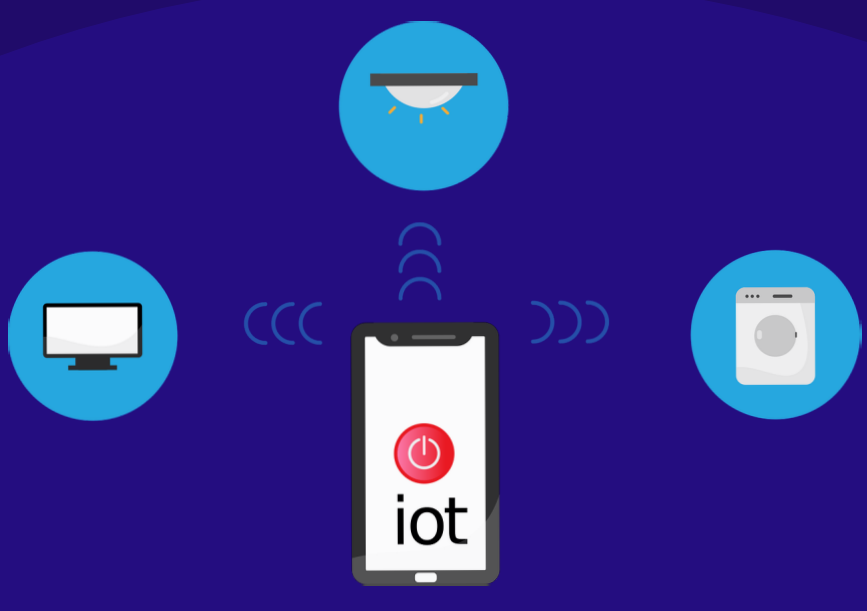
Malware may be injected into IoT through unsecured open ends like open ports, USB connectors, mobile charging ports, etc. Hackers gain access to storage media & data by physical tampering of devices.



Weak web interfaces like exposure of credentials in network traffic increase the possibility of a cyber attacker gaining unauthorized access to the network used for interacting with IoT devices.

If the devices have outdated protocols and are not being updated regularly, they can be compromised easily. Try to fix bugs in the system and install regular system updates over-time.

Unencrypted data leads to tampering and modification while data transmission. This is largely prevalent due to poor implementation of Security Sockets Layer/ Transport Layer Security.



www.centextech.com

Centex Technologies

CENTEX TECHNOLOGIES

13355 Noel Road,
Suite # 1100, Dallas, TX 75240

Phone: (972) 375 - 9654

501 N. 4th Street,
Killeen, TX 76541

Phone: (254) 213 - 4740

1201 Peachtree St NE,
Suite 200, Atlanta, GA 30361

Phone: (404) 994 - 5074

7600 Chevy Chase Drive,
Suite 300, Austin, TX 78752

Phone: (512) 956 - 5454

Image Source: Designed by Freepik