

IoT Threats and Risks

Network {Weak Encryption}
Malicious SSL Certificates
Packet/Session Sniffing
Man-in-the-Middle Attacks
DNS Cache Poisoning
Rogue Firmware
Eavesdropping
Location Tracking

Network Layer

Cloud Specific:
Insufficient Authentication for User and Device
Cross-Site Scripting {XSS}
Lack of Input Validation
Brute Force Attacks
Denial-of-Service
SQL Injection
Remote Command Execution
Privilege Escalation
Platform Vulnerabilities
Misconfigurations on Server
Lack of Disclosure on Compromises



Man-in-the-Middle Attacks
Escalated Privileges
Misconfiguration
Storage of Sensitive Data
Insufficient Encryption
Lack of SSL Validation
Phishing
Buffer Overflows
Caching of Data
Malware

Application Layer

Runtime Validation of Code/OS
Embedded Passwords
Insufficient Encryption
Unvalidated Code
Duplicate Identifiers
Forged Chips
Frequency of Patch Updates
Device/Sensor Cloning
Fake Device
Compromised 3rd Party Libraries

Device Layer