



Ministry of Electronics &
Information Technology
Government of India



National Centre
of Excellence
Cybersecurity Technology
And Entrepreneurship



CYBERSECURITY
CENTRE of EXCELLENCE
A joint initiative of DSCI & Government of Telangana

IoT SECURITY BEST PRACTICES



Table of Contents

SINTEKNO

01. What is IoT?	03
02. What is IoT Security?	04
03. Challenges in IoT security	05
04. OWASP IoT Security Project	07
05. Need for Best Practices and Best Practices for securing IoT	12
5.1 Consumer IoT Security Best Practices	12
5.2 Industrial IoT Security Best Practices	15
5.3 Cloud IoT Best Practices	16

The Internet of Things (IoT) is a network of interconnected computing devices, mechanical and digital tools, products, animals, or humans with unique IDs and has the capacity to transfer data without needing human-to-human or human-to-computer contact. As these devices range in complexity from common household items to sophisticated industrial instruments, experts have predicted that by 2025, there will be 22 billion linked IoT devices, up from more than 10 billion currently.

IoT devices can be operated from a smartphone, from a lightbulb to a car. Some bigger things, such as a jet engine, maybe loaded with hundreds of sensors that gather and send data to ensure that runs efficiently. On a larger scale, smart city initiatives involve blanketing entire regions with sensors to aid in our understanding and management of the environment.

With the help of the Internet of things, people may lead smarter lives, make better decisions, and exert total control over their surroundings. IoT is critical to business in addition to providing connected devices to automate homes. It gives firms a real-time view of how their systems work, providing insights into everything from machine performance to supply chain and logistic support operations.

The Internet of Things allows businesses to automate strategies and cut labor costs. It also reduces the amount of waste and helps to improve the quality, making manufacturing and delivery of goods less expensive, as well as providing transparency into transactions processed.

Different technologies that enabled IoT:

- Sensor
- Connectivity
- Cloud computing platform
- Machine learning
- Artificial Intelligence

Industries using IoT applications:

- Manufacturing
- Automotive
- Transportation and logistics
- Retail
- Public Sector
- Healthcare

WHAT IS IoT SECURITY?

IoT security encompasses both physical device and network security, and it affects the mechanisms, technological advances, and measures required to protect IoT systems and sensors. It includes industrial equipment, intelligent utility layouts, building automation systems, media devices, and other devices that aren't always built for network security.

However, any device linked to the Internet will be attacked. Attackers can use several tactics to remotely infiltrate IoT devices, including credential theft and exploiting vulnerabilities. They can utilize an IoT device to steal data, launch distributed denial-of-service (DDoS) attacks, or try to compromise the rest of the linked network once they have control of it.

There are sectors where IoT security is critical. Because of the extended attack surface of dangers that have already plagued networks, IoT security is crucial.

Threats involved:

Vulnerabilities

Vulnerabilities regularly confront consumers and companies with significant challenges. Several significant reasons IoT applications are insecure is that they lack the processing power necessary for security. Another factor contributing to widespread vulnerabilities is a restricted budget for designing and testing safe firmware, determined by device prices and development cycles.

Malware

Malware can infect IoT devices despite their minimal computer capacity. This has been a popular tactic among cyber criminals in recent years. And they're both flexible and beneficial for hackers; IoT botnet malware is one of the most commonly seen kinds.

Connected devices

Connected devices like all the rest involving the internet, it enhances the likelihood of online exposure. These gadgets may unwittingly store and target sensitive technology and confidential/personal information.

Weak Authentication

Weak Authentication IoT equipment (like home routers) is frequently released with simply discoverable credentials, that both suppliers and end users are free to leave in place. Such appliances are easy targets for attackers using automated scripts for mass exploitation when left accessible to remote access.

Device update management

Device update management hardware, or software can potentially be one of the most significant sources of software security threats. On the other hand, a manufacturer can provide the most recent product upgrades with the equipment he sells. There's a chance that these updates will result in certain security breaches.

Lack of Updates

If devices are launched with a defect that generates vulnerabilities, this is a significant IoT security risk. Manufacturers must be able to change their firmware to avoid these dangerous scenarios, whether they come from their code or code produced by a third party. This would be great if it could be done remotely, but that isn't always practical.

Lack of awareness

Individuals are often more aware of the importance of virus scans, as well as the importance of avoiding reading spam emails. However, because the Internet of Things is a relatively new technology, many people are confused about its principles and capabilities. As a result, IoT devices can represent major security concerns to manufacturers, users, and businesses. Hackers attack both people and devices. Some people have just rudimentary knowledge of electronics.

Weak Interfaces

Weak Interfaces data is processed and sent by every IoT device. Applications, resources, and standards are required for communication, and unsecured interfaces are the source of many IoT security updates. Weak device validation and weak or no encryption are two of the most common interface issues.

Untrustworthy connection

Many IoT devices communicate with the network without encryption. Currently, it is one of the most severe IoT security issues that exists.

Low Processing power

Low Processing Power IoT apps only need a small amount of data to function. This saves money and extends battery life, making OTA updates difficult and preventing the device from using security features like firewalls and virus scanners. As a result, they're more vulnerable to cyber-attacks. At this stage, security measures must be embedded into the network itself.

Connected Cars

Connected cars in addition to house invasion the IoT also poses a threat to your automobile. With the aid of linked IoT devices, smart automobiles are on their way to becoming a reality. However, because of its IoT connection, it has a greater danger of auto theft.

At the same time, there have been several instances of IoT systems being hacked due to cybercriminals successfully searching for IoT security weaknesses. Industrial robots, as well as the equipment attached to them, have been hacked in some cases. This is because hackers can change control-loop settings, interfere with production algorithms, and change the machine's status, among other things. This is why it is critical to secure IoT devices to avoid being a victim of cybercrime.

The OWASP Internet of Things Project was started in 2014 as a way to help Developers, Consumers, Manufacturers, and Enterprises to make better decisions regarding the creation and use of IoT systems. IoT Top 10 represents the top ten things to avoid when building, deploying, or managing IoT systems in terms of security. This is a unified list that captures the top things to avoid when dealing with IoT Security instead of separate lists for risks vs. threats vs. vulnerabilities —or developers vs. enterprises vs. consumers.

OWASP published its Top 10 List in 2018, and below are the top 10 Vulnerabilities identified.

1. Weak, Guessable, or Hardcoded Passwords

The use of easily brute-forced, unchangeable, or publicly available credentials and backdoors in client software or firmware that permit unauthorized access to deployed systems.

2. Insecure Network Services

Insecure network services running on the device, particularly those connected to the internet, jeopardize information confidentiality, integrity, and availability.

3. Insecure Ecosystem Interfaces

Outside of the device, the ecosystem's backend API, cloud, insecure web, or mobile interfaces allow the device compromise. Lack of authentication/authorization, weak encryption, and a lack of input and output filtering are all persistent problems.

4. Lack of Secure Update Mechanism

Lack of secure update mechanism is the inability This involves a lack of firmware validation on one device, a lack of secure delivery, anti-rollback mechanisms, and a lack of security change notifications due to updates.

5. Use of Insecure or Outdated Components

Use of obsolete or insecure software components or libraries, can make the device vulnerable. This includes insecure operating system platform customization and the use of third-party hardware or software components from a tainted supply chain.

6. Insufficient Privacy Protection

User's personal information is stored on the device or in the ecosystem that is used insecurely, improperly, or without permission.

7. Insecure Data Transfer and Storage

Inadequate encryption or access control for sensitive data anywhere in the ecosystem, including one at rest, in transit, and during processing.

8. Lack of Device Management

Lack of security support on production-ready devices, including asset management, system monitoring, update management, secure decommissioning, and response capabilities.

9. Insecure Default Settings

Devices or systems shipped with vulnerable default settings or inhibit operators from modifying configurations to make the system more secure.

10. Lack of Physical Hardening

Inadequate physical hardening measures allow potential attackers to obtain sensitive information that could be used in a future remote attack or to take local control of the device.

OWASP IoT Vulnerabilities and Attack Surface Mapping

Vulnerability	Attack Surface	Summary
Username Enumeration	• Administrative Interface • Device Web Interface • Cloud Interface • Mobile Application	• Ability to collect a set of valid usernames by interacting with the authentication mechanism.
Weak Passwords	• Administrative Interface • Device Web Interface • Cloud Interface • Mobile Application	• Ability to set account passwords to '1234' or '123456' for example. • Usage of pre-programmed default passwords.
Account Lockout	• Administrative Interface • Device Web Interface • Cloud Interface • Mobile Application	• Ability to continue sending authentication attempts after 3 – 5 failed login attempts.

Vulnerability	Attack Surface	Summary
Unencrypted Services	• Device Network Services	• Network services are not properly encrypted to prevent eavesdropping or tampering by attackers.
Two-factor Authentication	• Administrative Interface • Cloud Web Interface • Mobile Application	• Lack of two-factor authentication mechanisms such as a security token or fingerprint scanner.
Poorly Implemented Encryption	• Device Network Services	• Encryption is implemented however it is improperly configured or is not being properly updated, e.g. using SSL v2.
Update Sent Without Encryption	• Update Mechanism	• Updates are transmitted over the network without using TLS or encrypting the update file itself.
Update Location Writable	• Update Mechanism	• Storage location for update files is world writable potentially allowing firmware to be modified and distributed to all users.
Denial of Service	• Device Network Services	• Service can be attacked in a way that denies service to that service or the entire device.
Removal of Storage Media	• Device Physical Interfaces	• Ability to physically remove the storage media from the device.

Vulnerability	Attack Surface	Summary
No Manual Update Mechanism	Update Mechanism	No ability to manually force an update check for the device.
Missing Update Mechanism	Update Mechanism	No ability to update device.
Firmware Version Display and/or Last Update Date	Device Firmware	Current firmware version is not displayed and/or the last update date is not displayed.
Firmware and storage extraction	- JTAG / SWD interface - In-Situ dumping - Intercepting a OTA update - Downloading from the manufacturers web page - eMMC tapping - Unsoldering the SPI Flash / eMMC chip and reading it in a adapter	Firmware contains a lot of useful information, like source code and binaries of running services, pre-set passwords, ssh keys etc.
Manipulating the code execution flow of the device	- JTAG / SWD interface - Side channel attacks like glitching	- With the help of a JTAG adapter and gdb we can modify the execution of firmware in the device and bypass almost all software based security controls. - Side channel attacks can also modify the execution flow or can be used to leak interesting information from the device.

Vulnerability	Attack Surface	Summary
Obtaining console access	Serial interfaces (SPI / UART)	- By connecting to a serial interface, we will obtain full console access to a device. - Usually, security measures include custom bootloaders that prevent the attacker from entering single-user mode, but that can also be bypassed.
Insecure 3rd party components	Software	Out-of-date versions of busybox, openssl, ssh, web servers, etc.

Source: https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Vulnerabilities

OWASP top 10 IoT Vulnerabilities

A successful IoT security plan must include the security controls that must be installed, as well as how they will be monitored and revised over time. To guarantee that the overall premises are safe against IoT threats, it must also provide in-depth insight into the organization's IT infrastructure and endpoints.

Best practices for IoT security include:

- IoT Endpoint Protection
- IoT Gateway Security
- Security Cloud API
- Developing Secure Network
- Up-to-date Data Encryption
- Protected Data Storage
- Update to Identity-level protocol
- Implement Patching and Remediation

The rapid growth of IoT devices and their adaptation raises an equally serious security problem. The more internet-connected gadgets you have, the more ways bad actors may get into your network. To be secure, both consumers and companies should plan ahead of time for this transition. There are various recommended standards for the IoT listed above that may help safeguard your data in the future.

5.1 Consumer IoT Security Best Practices

5.1.1 Ensure Unique Credentials

Many IoT devices come with global default usernames and passwords that the consumer is supposed to alter. During device provisioning, every IoT device's default passwords must be unique per device or require the user to specify a password that follows the best standards. There must be no way to reset the passwords to a global default setting. It has been the root of a slew of IoT security vulnerabilities, and it's time to end it. Best practices for passwords and other authentication mechanisms should be followed, such as using the strongest password feasible that is acceptable for the device's usage context. Associated online services should use multi-factor authentication, and no superfluous user information should be exposed before authentication. Every password reset procedure should ensure that the user is properly authenticated.

5.1.2 Store credentials and security-sensitive data securely

Any credentials that are saved within services must be kept safe. Credentials that are hard-coded in software are not allowed.

5.1.3 Validate input data

Validation is required for data input via user interfaces and data transmission via APIs or between networks in devices and services.

5.1.4 Implement a vulnerability disclosure policy

As part of a vulnerability disclosure policy, all organizations that supply internet-connected devices and services must give a public point of contact for security researchers and others to report concerns. Vulnerabilities should be addressed as soon as possible in a documented and published procedure.

5.1.5 Keep Software Up to Date

Software in devices with internet connectivity should be dynamic and change securely. Updates must be made promptly and should not interfere with the device's operation. For end-point devices, an end-of-life policy must be published that specifies the minimum time a device will get software updates and the reasons for the length of the support term. Consumers should be informed about the importance of each update, which should be simple to execute. The product should be isolatable and replaceable for constrained devices that cannot be physically upgraded.

5.1.6 Secure Communication

Data sensitive to security breaches, including any remote management and control, should be encrypted in the transmission according to the technology's and usage's attributes. All keys should be kept in a safe place.

5.1.7 Minimise Exposed Attack Surface

All devices and services should follow the 'principle of least privilege,' which means that unused ports should be closed, hardware shouldn't expose access unnecessarily, services shouldn't be available if they aren't used, and code should be kept to the minimum functionality required for the service to function. Software should be run with the necessary permissions, considering security and functionality.

5.1.8 Ensure Software Integrity

Secure boot procedures should be used to verify the software on IoT devices. If an unauthorized modification is identified, the device should notify the user/administrator of the problem and not connect to any networks other than those required to conduct the alerting function.

5.1.9 Ensure the protection of personal data

When services or devices process personal data, they must comply with applicable data protection legislation, such as the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. For each device and service, device makers and IoT service providers must offer users open and unambiguous information about how their data is utilized, by whom, and for what objectives. This includes any other parties that could be involved. When personal data is handled with consumers' consent, it must be collected in a legal and authorized manner, with those consumers having the right to withdraw their consent at any time. Suppose a mechanism like Blockchain is used for data collection, where it is not possible to erase the data permanently due to the inherent nature of the design of such systems. In that case, the consumers must be made aware of the situation before getting their permission so that they are well informed about the consequences of their data on external systems.

5.1.10 Make systems resilient to outages

Where their use or other depending systems necessitate it, resilience should be integrated into IoT devices and services, considering the potential of data network and power outages. In the event of a network outage, IoT services should stay operational and locally functional as much as feasible and should recover. In the event of a power outage, cleanly restore electricity. Instead of a vast scale reconnect, devices should be able to re-join a network in a smart and orderly manner.

5.1.11 Monitor system telemetry data

If a dataset, such as use and measurement data, is gathered from IoT devices and services, it should be checked for security irregularities.

5.1.12 Make it easier for customers to delete personal data

Personal data shall be readily deleted from devices and services in the event of a change of ownership, when the consumer decides to erase it, or when the consumer wishes to dispose of the device. Precise information on how to erase personal data should be provided to consumers. Consumers must be cautioned whenever a data deletion process is initiated, and the erased data should be permanently irrecoverable.

5.1.13 Make installation and maintenance of device easy

IoT device installation and maintenance should take only a few steps and adhere to security best practices for usability. Consumers should also be given instructions on how to set their devices safely.

5.2 Industrial IoT Security Best Practices

5.2.1 Network Segmentation

To access a network shared by office PCs and IIoT equipment, the attacker can use phishing emails or malware to deceive employees. A possible concern is that attackers might use other devices on the network to obtain access to industrial settings. In the network, IIoT systems must be properly isolated. As a result, devices and sensors that control pumps, valves, or any other SCADA system component should always be connected to a separate network from the rest of the IT infrastructure.

5.2.2 Weigh the risks of melding IT and OT

IIoT requires both IT and OT to function successfully. Both of them, however, have very different goals and objectives. OT is concerned with quality, yield, and efficiency, whereas IT is concerned with infrastructure, security, and governance [Fo17]. In addition, IT and OT have separate security techniques, assessing various threats, focusing on different patching cycles, protocols, and so on.

5.2.3 Appropriate Access Controls Schemes and Granularity

The granularity of today's OT systems is frequently quite coarse. This might be for practical reasons, such as enabling security at the transport layer with OPC UA while giving all clients full access to a single server. Current systems often have role-based access control (RBAC) methods as well as the ability to choose groupings of data (for example, set-points) that may be accessed read-only or read-write. With an essential infrastructure accessible through the internet, a tighter access control granularity paired with access constraints, as offered by Attribute-Based Access Control (ABAC) methods, can provide a better level of safety.

5.2.4 Secure Interoperability

According to the German Standardization Roadmap for Industry 4.0 [Ge18], OPC Unified Architecture (OPC UA) is the fundamental interoperability standard for the deployment of Service Oriented Architecture (SOA) in Industry 4.0. The multipart standard IEC 62541 defines this platform-independent, scalable protocol. The security model for OPC UA is described in IEC 62541-2 [IEC02]. It is also crucial for IIoT systems that use this protocol to enable and enforce the security features that come with it. This is an issue since the protocol may be used for Machine-to-Machine communication across various firms' factories and plants and IIoT devices in different countries.

5.2.5 Have an emergency response team in place

Establishing an emergency response agency, formulating an emergency response strategy, and establishing human resource measures such as an expert resource pool and a supporting manufacturer's resource pool are all things that businesses must do. Similarly, emergency drills must be conducted regularly so that all key partners know what to do in the case of an emergency.

5.2.6 Secure and Preventive Maintenance Procedures Preparation

Factories and asset owners can benefit from preventive maintenance to reduce losses and business interruptions. With internet access to factories and facilities, most preventative maintenance may be started from the OEM's or Systems Integrator's offices. This allows OEMs and integrators to do preventative maintenance in ways that were not possible before the rollout of IIoT devices. When permitting preventative and recurring maintenance (e.g., via over the air) of application software and Firmware upgrades, security considerations must be considered.

5.3 Cloud IoT Best Practices

The cloud has turned out to be an exceptionally popular area for developers to place IoT systems and devices. In today's smart world, IoT security is a significant challenge.

The best IoT security results are embedded in cloud security. Integrating cloud security in IoT provides a foundation for managing security provisions and offers intrinsic security practices.

Following are the best practices for ensuring IoT Cloud security:

To access a network shared by office PCs and IIoT equipment, the attacker can use phishing emails or malware to deceive employees. A possible concern is that attackers might use other devices on the network to obtain access to industrial settings. In the network, IIoT systems must be properly isolated. As a result, devices and sensors that control pumps, valves, or any other SCADA system component should always be connected to a separate network from the rest of the IT infrastructure.

5.3.1 Introducing planned defensive measure methodology

Step 1: Build an incident management procedure that aligns to your organizational needs.

Step 2: Developing incident response simulations and usage of automation tools to improve the rate of investigation and detection speed by minimizing recovery time.

5.3.2 Updating passwords on Cloud-based devices at regular intervals

There is a high chance of attackers accessing the intelligent devices stored on the cloud and retrieving the password. Henceforth, the best idea is to not only secure the password by changing it often but also set up a two-factor authentication mechanism as an extra line of defence strategy. This can be done by combining the secret key (password) with a one-time code transferred via a secondary mode of channel line (mobile text message) or via any token generator application.

5.3.3 Initialize traceability

Need to set up a critical action plan for monitoring, alerting, and auditing to adapt the changes to real-time environment. This can be done by integrating logs and metrics with systems to respond and act regularly.

5.3.4 Keep Authentication Keys Safe

Always ensure that all the IoT encryption algorithms and keys are secure. An authentication method must be set up to identify the individuals accessing the data stored in the cloud. Moreover, as security is our highest priority, it is critical to make sure that a copy of these authentication keys is in secure storage.

5.3.5 Securing all the layers

Instead of safeguarding only the outer layers, we need to consider all the layers and implement a defense-in-depth methodology along with security controls. Consider all layers and their surrounding perimeter (e.g., operating system, subnet, virtual private cloud (VPC), every instance, load balancer, edge network, and application).

5.3.6 Mechanisms to safeguard data and eliminate risks

Create access control, encryption, and tokenization procedures for securing the data at rest and transit and apply these methods appropriately. Also, introducing tools with a proper plan will lower the risks of data loss, reduce the need for manual and direct data processing, and minimize the chance of human error when sensitive data is modified.

References:

You can consult the [IoT Security Guidelines book](#), produced by CCoE, for further details on various security elements, guidelines, and their security standards.