This document presents the data cataloged in the studies carried out (ad-hoc and structured literature review). The access links to the pages identified in the Ad-hoc process will be listed below, while the works cataloged in the structured review can be found in the technical report available at that same link.

OWASP Internet of Things Project - OWASP

IoT Product Criteria | NIST

Top IoT Device Vulnerabilities: How To Secure IoT Devices | Fortinet

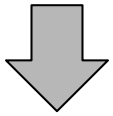
These new vulnerabilities put millions of IoT devices at risk, so patch now | ZDNet

The real dangers of vulnerable IoT devices - Infosec Resources (infosecinstitute.com)

The Main Vulnerabilities and Security Risks within IoT Devices (linkedin.com)

The Most Important Security Problems with IoT Devices (eurofins-cybersecurity.com

The identified vulnerabilities are listed on the following pages along with their respective descriptions.



Vulnerabilities Ad-hoc	Description
Insecure Data Transfer and Storage	Data that IoT devices receive or transmit over networks needs to be secured and restricted from unauthorized users. This is critical to maintaining the integrity and reliability of IoT applications and organizations' decision-making processes.
Weak Passwords	Weak or hardcoded passwords are among the most frequent methods attackers use to compromise IoT devices. Weak, reused passwords that are short or easy to guess are simple for attackers to crack, which they use to compromise devices and launch large-scale attacks.
Insecure Update Mechanisms	Devices with insecure update processes are at risk of installing malicious or unauthorized code, firmware, and software. Corrupt updates can compromise IoT devices, which can be critical for organizations in the energy, healthcare and industrial sectors. Updates need to be secure and on encrypted channels, while all software must be validated and approved.
Insufficient Physical Security	If attackers have physical access to a device, they can open the device and attack the hardware. For example, by reading the contents of memory components directly, any protection software can be bypassed. In addition, the device may have debug contacts, accessible after opening the device, which provide an attacker with additional possibilities.
Insufficient Privacy Protection	User personal information stored on the device or ecosystem that is used insecurely, inappropriately, or without permission.
Lack of Device Management	One of the most challenging tasks to minimize risk is managing all the devices and closing the perimeter. Device scanning and profiling allows security teams to gain visibility into their IoT devices across networks, thus considering their risks, behavior, activity, and so on.
Insecure Network Services	Unnecessary or insecure network services that run on devices, particularly those that are exposed to the internet, jeopardize the availability of confidentiality, integrity/authenticity of information, and open up the risk of unauthorized remote control of IoT devices. Unrequired open ports and services that transmit information over your networks should be inspected and consider removing or disabling as a security measure (if not required).
Insecure Ecosystem Interfaces	Insecure ecosystem interfaces such as application programming interfaces (APIs) and mobile and web apps allow attackers to compromise a device. Organizations need to implement authentication and authorization processes that validate users and secure their cloud and mobile interfaces. Handy identity tools help the server differentiate valid devices from malicious users.
Manipulating the code execution	With the help of a JTAG adapter and gdb we can modify the firmware running on 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 device information

Lack of encryption	When a device communicates in plain text, all information being exchanged with a client device or backend service can be obtained by a 'Man in the Middle'. Anyone who is able to get a foothold on the network path between a device and its endpoint can inspect network traffic and potentially obtain sensitive data such as login credentials. Even when data is encrypted, weaknesses can be present if encryption is not complete or configured incorrectly.
Application vulnerabilities	Recognizing that software contains vulnerabilities in the first place is an important step in securing IoT devices. Software bugs can make it possible to trigger functionality on the device that was not intended by the developers. In some cases, this could result in the attacker running their own code on the device, making it possible to extract sensitive information or attack other parties.
Incorrect access control	The services offered by an IoT device should only be accessible by the owner and people in their immediate environment whom they trust. However, this is often insufficiently enforced by a device's security system. IoT devices can trust the local network to such a degree that no further authentication or authorization is required.
Intrusion ignorance	When a device is compromised, it often continues to function normally from the user's point of view. Any additional bandwidth or power usage usually goes undetected. Most devices do not have logging or alerting functionality to notify the user of any security issues.
Lack of Trusted Execution Environment	Most IoT devices are effectively general-purpose computers that can run specific software. This makes it possible for attackers to install their own software that has functionality that is not part of the normal functioning of the device. By limiting the device's functionality and the software it can run, the possibilities of abusing the device are limited. To limit the software a device can run, code is typically signed with a cryptographic hash.
Outdated software	As vulnerabilities in software are discovered and resolved, it is important to distribute the updated version to protect against the vulnerability. This means that IoT devices must ship with updated software without any known vulnerabilities, and that they must have update functionality to fix any vulnerabilities that become known after device deployment.
Overly large attack surface	Every connection that can be made to a system provides a new set of opportunities for an attacker to discover and exploit vulnerabilities. The more services a device offers over the Internet, the more services it can attack. This is known as the attack surface. Reducing the attack surface is one of the first steps in securing a system.
User interaction	Vendors can encourage secure deployment of their devices by making it easy to configure them securely. By paying due attention to usability, design, and documentation, users can be encouraged to configure secure configurations.

Vendor security posture	When security vulnerabilities are found, the vendor's reaction greatly determines the impact. The vendor has a role to receive information about potential vulnerabilities, develop a mitigation and update devices in the field. The vendor's security posture is often determined by whether the vendor has a process in place to properly handle security issues.
Insecure Default Settings	IoT devices, like personal devices, come with default, hard-coded configurations that allow for simple configuration. However, these default settings are highly insecure and easy for attackers to crack. Once compromised, hackers can exploit vulnerabilities in a device's firmware and launch broader attacks against businesses.
Insecure or Outdated Components	The IoT ecosystem can be compromised by code and software vulnerabilities and legacy systems. The use of insecure or outdated components, such as open source code or third-party software, can introduce vulnerabilities that expand an organization's attack surface.
TCP/IP Stacks	Vulnerabilities affecting TCP/IP stacks – communication protocols commonly used in IoT devices – relate to Domain Name System (DNS) implementations, which can lead to Denial of Service (DoS) or RCE (Remote Code Execution) by attackers .
Account Lockout	Ability to continue sending authentication attempts after 3 - 5 failed login attempts
Insecure 3rd party components	Outdated versions of busybox, openssl, ssh, web servers, etc.
Obtaining console access	By connecting to a serial interface, we will gain full console access to a device. Security measures often include custom bootloaders that prevent the attacker from entering single-user mode, but these can also be bypassed.
Lack of Two-factor Authentication	Lack of two-factor authentication mechanisms like a security token or fingerprint scanner
Update Location Writable	Storage location for update files is world-writable, allowing firmware to be modified and distributed to all users
Username Enumeration	Ability to collect a set of valid usernames by interacting with the authentication mechanism

Vulnerabilities Structured Review	Category	Description
Broken Authentication	Application	The process of confirming the identity or veracity of an object is known as authentication. With many IoT devices in smart environments lacking strong authentication or access control mechanisms, it becomes easy for attackers to impersonate a legitimate user and use the credentials or any other information that gives them access to exploit and uncover security holes in web applications.
Buffer Overflow	Application	Buffer overflow occurs when a program or process attempts to write more data to a fixed-length block of memory, or buffer, than the buffer was designed to hold
Data Inconsistency	Application	In IoT, attack on data integrity leading to inconsistency of data in transit or data stored in a central database is referred to as Data Inconsistency
Insecure Access Management	Application	Access control is necessary to prevent unauthorized entities from gaining access to system's resources, and to ensure that authorized entities can only access the resources they are allowed to access. Therefore, reliable access control policies play a major role in preventing activities that lead to a breach of security in the IoT.
Insecure Interface Configuration	Application	Web interfaces are commonly used to interact with IoT devices, allowing users to access and control their features and settings through a browser. However, if these interfaces are not adequately secured, they can pose a significant security risk. Lack of security in an IoT web interface can lead to several vulnerabilities, including weak passwords or predictable patterns, encryption issues, authentication flaws, outdated software, and lack of access control.
Insecure Management of Data	Application	Management of data is also vital to protect and manage that data so that the authorized objects will get their data. In any IoT smart environment, without proper security mechanisms that protect data and information from malware and other malicious intruders, personal information could easily be leaked resulting in security breaches
Insecure Software	Application	Software updating is a process that should never fail or be compromised in an IoT-based system. Attention should be paid to insecure update processes that risk installing malicious or unauthorized software, with corrupt updates that can compromise IoT devices. You should avoid using insecure or outdated components, such as open source or third-party software. However, manually updating patches for each IoT device may not be feasible.
Lack of Active Device Monitoring	Application	Monitoring IoT devices can be challenging. This is because most existing monitoring tools and practices, especially those with a cloud focus, have traditionally been designed to monitor time-series metric data with no focus on modern IoT devices or their processes. The lack of active IoT device monitoring tools makes it difficult to achieve full network visibility in IoT-based smart environments.
Low Quality Level Code	Application	The level of low-quality code in IoT environment applications refers to the presence of software development practices that result in poorly structured source code with potential security and reliability issues through improper use of features that result in security flaws such as lack of input validation, improper password handling, or weak encryption, which can facilitate attacks.
Non-repudiation	Application	In a general information security context, assurance that the sender of information is provided with proof of delivery, and the recipient is provided with proof of the sender's identity, so neither can later deny having process the information .
SQL Injections	Application	This is one of the most known vulnerability points for servers that accept SQL queries and updates, where additional commands can be injected to steal database information or change/delete database records. In this type of attack, many attackers use SQL statements to write, delete operations, and read when the web application is being invaded by SQL injection
Weak/lack In-app Encryption	Application	Weak or absent encryption in IoT system applications refers to the lack of proper implementation of encryption algorithms or the use of encryption algorithms that are considered weak and easily breakable. Encryption is an essential measure to protect the confidentiality, integrity, and authenticity of data transmitted and stored in IoT systems.
Malicious code in-app	Application	Malicious code in IoT system applications refers to software programs or code snippets that have been developed with malicious intent and are designed to compromise the security, privacy, or proper functioning of IoT devices and related systems.

Systems Low-cost	Device	Because the firmware/operating systems used by low-cost IoT devices might not have been as robustly tested as desktop/server operating systems, the boot process might be exploited to compromise the device
Channel Voice	Device	In the smart home, this information may now be picked up more easily by exploiting poorly protected IoT devices with built-in microphone systems, such as personal assistant services (e.g., Google Home, Amazon Echo), children toys and other voice-controlled house-hold appliances. These systems are vulnerable to attacks like voice squatting and voice masquerading.
Default Configuration	Device	Many times the default settings that are assigned by the device manufacturers benefit the company rather than its users. Manufacturers often add or enable features that are not essential in the operation of the device that aids attackers in launching their attacks. These settings should be checked and changed immediately after the device is purchased and setup. The default login settings of IoT devices may be used by the attackers to access the device illicitly, or to reset the password.
Device Spoofing	Device	Device spoofing refers to a technique in which an attacker disguises their device to appear as a legitimate or trusted device on a network or system. The purpose of device spoofing is to deceive network administrators, security systems, or other devices into granting unauthorized access or privileges to the attacker. In device spoofing, the attacker typically manipulates or forges identifying information, such as MAC addresses, IP addresses, or device identifiers, to masquerade their device as another trusted device.
Electromagnetic Emanations Leaking	Device	electromagnetic emanation resulting from information processing within devices. The information gathering is based on observing the electromagnetic fields from the IoT devices. Here, an example would be the electromagnetic emanations leaking from unfiltered powerlines. There are demonstrations of the viability of measuring a home’s powerline activity with such accuracy that they could identify what the occupants were watching on television.
Energy Restraints	Device	Smart devices, like smartphones and sensing nodes, are responsible to collect data in smart cities and suffer from resource limitations, e.g., energy resources. The smart devices, such as IoT sensors, in the cloud-driven IoT-based big data environment may be failed due to energy issues or can be physically stolen by the adversary. Types of attacks will lead to battery-drained IoT devices being out of service.
Heterogeneous Interaction	Device	The vulnerability based on the heterogeneity of connected and interaction IoT devices refers to the exploitation of security weaknesses that arise due to the diversity of IoT devices present in a connected environment. This heterogeneity encompasses differences in terms of hardware, software, communication protocols, and configurations among IoT devices.
Insecure Data Transfer and Storage	Device	The vulnerabilities present in each layer would not be able to transfer the data securely and also the data can be corrupted by the hacker due to its several attacks in IoT. Management of data is also vital to protect and manage that data so that the authorized objects will get their data. The data generated at the hardware is modified, which can set off an absolute difference in the data, further sent to higher layers for processing. This is because the IoT devices, which are in charge of collecting and transferring data, are vulnerable to a wide variety of attack forms. For example, the injection of fake, erroneous, or erratic sensor data are the forms of attacks into the IoT systems, which are able to redirect decisions of the automated system to behave in the attacker's desired manner.
Insecure Firmware	Device	IoT devices consisting of software and hardware are less in numbers and due to heterogeneous nature, firmware is not updated frequently that causes a variety of security threats
Insecure Initialization	Device	To ensure a proper and secure network service in IoT, we must initialize and con?gure IoT devices in the physical layer without deviating secrecy and obstacle to the network.
Insecure Password	Device	A security weakness occurs when passwords are weak, weak, guessable, defaults, shared or stored improperly. Passwords are a standard mechanism for authentication and protection in computer systems and applications. Still, when poorly chosen or managed, they can allow unauthorized access to sensitive accounts, devices, or information.
Insufficient Testing	Device	Most of the IoT devices are produced quickly to meet the increasing market demands and hence do not undergo proper testing or follow any acceptable security standards or assessment frameworks. devices might not have been as robustly tested as desktop/server operating systems.

Lack of Side Channel Protection	Device	A side-channel attack refers to attacks that result in revealing useful information regarding the transmitted data or the internal working of the system through alternative paths. This attack attempts to retrieve information indirectly and mainly exploit information leakage. Examples of side-channel attacks include capturing and analysing timing information, power consumption, electromagnetic leaks, acoustic signal analysis and data remanence
Lack of Strong Authentication	Device	In the IoT, an authentication protocol should be developed to confirm mutual trust between different objects, users, or systems by verifying their identities. Allow an attacker to access the device without providing the correct credentials, bypassing authentication mechanisms, and gaining control over the device.
Low Computing Power	Device	IoT devices typically have limited resources, which means they would have to rely on less robust operating systems and network protocols, and hence, may be easier to compromise. On the other hand, they collect sensitive information, which would aggravate the risk. The limited processing capability, traditional security methods suffer from various setbacks and often do not detect the physical threats in the network
Low Data Transmission Range	Device	Devices with low data transmission range are susceptible to attacks because they require proximity to other devices to exchange data.
Malicious Code Injection	Device	Here the attacker injects malicious code onto a physical device by compromising it which may help him/her launch other attacks too. The attacker compromises a node by physically injecting it with malicious code that would give him access to the IoT system. An adversary aims to install a compromised version of the software/firmware during wireless updates of the IoT device, which could give the adversary full remote control over the compromised device.
Obtaining Console Access	Device	By connecting to a serial interface, we will gain full console access to a device. The attacker can access the hardware and read and modify the default settings of the IoT device, which can affect privacy and authentication credentials. intentional modification of the system circuitry configuration.
Physical Damage	Device	Physical damage to equipment can be natural as a result of calamity or otherwise. It can lead to null values at receiving end or missed values, which can cause an imbalance in the real-time processing of data. Ref. [ ]described how a drone can be controlled to take over and remotely cause failure to other nodes in its vicinity through an insecure channel.
Physical Tampering	Device	Refers to the act of physically modifying a device (e.g. RFID) or communication link. It is important to mention that an adversary can tamper with the device and use it to insert impostor to the system, use the device maliciously or out of its intended functionality. This type of attack is launched when the attacker is much closer to the network device and is forced to break hardware without any permission.
Sleep Deprivation	Device	Many IoT devices use battery as the power sources, hence, they only sense and transmit periodically and go to a sleep state in between. The aim of this attack is to somehow prevent the devices from going to sleep or to minimize the sleep period, thereby drain the batter much faster than normal usage
Tag Cloning	Device	Malicious activity in which an attacker duplicates or replicates an IoT device's unique identification tag in order to deceive or compromise the system. Tags are components used in technologies such as RFID (Radio-Frequency Identification) to identify and track devices or objects. Tag cloning at the physical layer involves taking the unique identification information from a legitimate tag and reproducing it in a spoofed tag.
Unprotected Physical Access	Device	Refers to the capturing of an IoT device physically. This threat could be serious if the IoT devices have to be deployed in areas without physical security protection.
Weak Access Control	Device	Access control is necessary to prevent unauthorized entities from gaining access to system's resources, and to ensure that authorized entities can only access the resources they are allowed to access. Therefore, reliable access control policies play a major role in preventing activities that lead to a breach of security in the IoT. [A taxonomy of security and privacy requirements for the Internet of Things (IoT)]
Weak/lack of Encrypt	Device	Weak or lack of encryption in IoT devices refers to a vulnerability where the encryption mechanisms in place for protecting data in transit or at rest within the devices are insufficient or completely absent.
Insecure physical interface	Device	Debugging exploits to negotiated nodes in the network by the poor physical security with the help of physical interface and tools

Channel Interference	Network	Jamming attacks are availability attacks against the wireless medium or the external facing sensors. Consequently, the authorized communication is disrupted. Sensors that may be susceptible to this attack, where a jammer device can be used to block the sensors from receiving signals.
Communication Overhead	Network	The total number of packets are to be transferred or transmitted from one node to another is known as the communication overhead. It includes the overhead of routing process, routing table and packet preparation in a sensor node.
Data Leak or Breach	Network	Refers to the leakage or breach of data in IoT networks through security holes that allow unauthorized access, disclosure or loss of confidential data transmitted or stored in IoT networks.
Eavesdropping	Network	Because the IoT devices are transmitting wirelessly, it is easier to intercept the transmitted signals even if the IoT devices are protected with physical security
Fake/Malicious Node	Network	Attacker drops a fake node between two legitimate nodes of the network to control data flow between them. Malicious IoT node could be connected to IoT system in order to collect and exchange data from other devices
Heterogeneous Communication	Network	Refers to the exchange of data and information between devices and systems that use different communication protocols, standards, or technologies within the network.
Insecure Server	Network	Refers to a server or backend infrastructure that is vulnerable to security threats and lacks adequate safeguards to protect the data and devices connected to the network. In IoT networks, servers play a critical role in handling data processing, storage, and communication between devices and applications.
Insecure Update Mechanisms	Network	The IoT connected resources have more demand for updating and the frequency of the messages causes latency which results in network vulnerabilities.
Lack of Proper Authentication Mechanisms	Network	Absence or inadequacy of mechanisms that verify the identity and permissions of entities, such as devices, users, or services, attempting to access or interact with the network. Authentication is a fundamental security mechanism that ensures that only authorized entities are granted access to the network and its resources
Lack of Strong Password	Network	Absence or inadequate use of robust and secure passwords for authentication and access control purposes within the network. Passwords serve as a primary means of verifying the identity of users, devices, or services attempting to access the IoT network or its resources
Lack Secure Communication Protocols	Network	The lack of secure communication protocols in IoT networks refers to the absence or inadequate use of protocols that ensure the confidentiality, integrity, and authenticity of data transmitted between IoT devices, services, and backend systems. If secure communication protocols are not in place, it introduces significant security risks.
Configure network repeatedly	Network	Security weakness that arises when network configurations are frequently applied or modified, potentially leaving the network exposed to unauthorized access, misconfigurations, or other security risks
Single-Point Dependency	Network	Security weakness arises when the network relies heavily on a single component, device, or service for its operation, making it susceptible to disruptions or compromise if that single point of dependency fails or is compromised. A single point of dependency refers to a critical component, device, or service that, if compromised or unavailable, can cause significant disruptions, loss of functionality, or even complete failure of the network
Spoofing Signal	Network	An attacker impersonates or forges a signal to deceive IoT devices, services, or networks into accepting unauthorized commands or providing sensitive information. Spoofing signals involve manipulating or mimicking the signals transmitted between devices or services to gain unauthorized access or manipulate the network.
Unauthorized Access	Network	Access control is necessary to prevent unauthorized entities from gaining access to system's resources, and to ensure that authorized entities can only access the resources they are allowed to access. Therefore, reliable access control policies play a major role in preventing activities that lead to a breach of security in the IoT.
Unsecured Network	Network	Keeping these devices in a separate private network also eliminates the possibility of an attacker infecting other devices and spreading the malware in the network when the device is connected to unsecured public Wi-Fi networks

Unused Ports Enable	Network	Unnecessary or unused network ports on IoT devices or network infrastructure are left enabled, potentially providing unauthorized access points for attackers. Unused ports are those that are not actively utilized for intended purposes in the IoT network.
Weak/lack Encryption in Communication	Network	refers to a security vulnerability that arises when the data transmitted between IoT devices or between devices and the network is not adequately protected with strong encryption mechanisms.
Physical properties of the power system	Network	Refers to security weaknesses that arise from the physical infrastructure and characteristics of the power supply system used to support IoT devices and networks. Power systems are essential for providing the necessary electrical energy to operate the devices and ensure their continuous functionality.
Wifi De-authentication	Network	WiFi de-authentication is by no means new, but in the context of the smart home, the loss of WiFi means loss of Internet connectivity in the household, on which IoT platforms are increasingly dependent in order to function. When an attacker maliciously de-authenticates or disconnects IoT devices from their Wi-Fi networks, leading to service disruptions, loss of connectivity, or potential unauthorized access to the devices or network. Wi-Fi de-authentication attacks exploit the communication protocol used by Wi-Fi networks to force devices to disconnect from their current network.
Insecure traffic control	Network	A firewall is a network security system that controls incoming and outgoing network trafic based on a set of rules. It is also relevant for AVs to have such segregation which acts as a barrier between the trusted network and other untrusted or less-trusted networks within the vehicle or in the V2V, V2I and V2IoT scenarios.
Centralized architecture	Network	IoT connected devices transmit compute requests and data information from their sensors directly back to the data center where information processing and storage is performed by servers running specific Apps through the switches. The requests for action and the processed data are in turn sent back to the connected devices from these centralized applications.
Access Malicious Link	Peopleware	Users click or interact with links designed to deceive or exploit them. Malicious links can be delivered through various channels, including email, social media, messaging platforms, or compromised websites
Identifying the Product Vendor	Peopleware	Identifying the product vendor allows attackers to analyze the smart home and target known vulnerabilities in its devices.
Knowledge the System	Peopleware	For the vulnerability of system knowledge, we have two reference points: the attacker's perspective, as they are aware of the system's weak points and employ malware or appropriate techniques for intrusion, and the user's perspective, considering the increasing innovation of IoT technologies, where many users still need to understand how modern IoT devices are designed and function in order to better protect themselves.
Lack of Technical Support	Peopleware	Absence or insufficient availability of resources, expertise, and assistance to address technical issues or provide guidance for IoT devices and networks. When there is a lack of technical support, IoT system users may encounter difficulties in setting up, configuring, troubleshooting, or maintaining their devices and networks
Personal and Social Circumstances	Peopleware	Refer to security failures that arise due to personal and social factors related to users, such as inappropriate behaviors, lack of awareness or training, negligence, or misuse of IoT devices.
Phishing	Peopleware	Phishing is used to trick people into entering their personal information or downloading malicious software that is capable of spreading malware. A malicious entity attempts to guide the user of the device to another server or for marketing purposes or to try to deceive to steal personal
Social Engineering	Peopleware	The attacker manipulates users of an IoT system, to extract private information. This makes it easy for attackers to use social engineering to trick IoT device users into providing sensitive data or information which can be used to gain access into smart environment networks
Untrusted Device Acquisition	Peopleware	Users or organizations acquire and integrate IoT devices into their networks without ensuring the trustworthiness or security of those devices.
Vendor Security Posture	Peopleware	When security vulnerabilities are discovered, the vendor's response greatly determines the impact. The vendor has a role to receive information about potential vulnerabilities, develop mitigation measures, and update devices in the field.