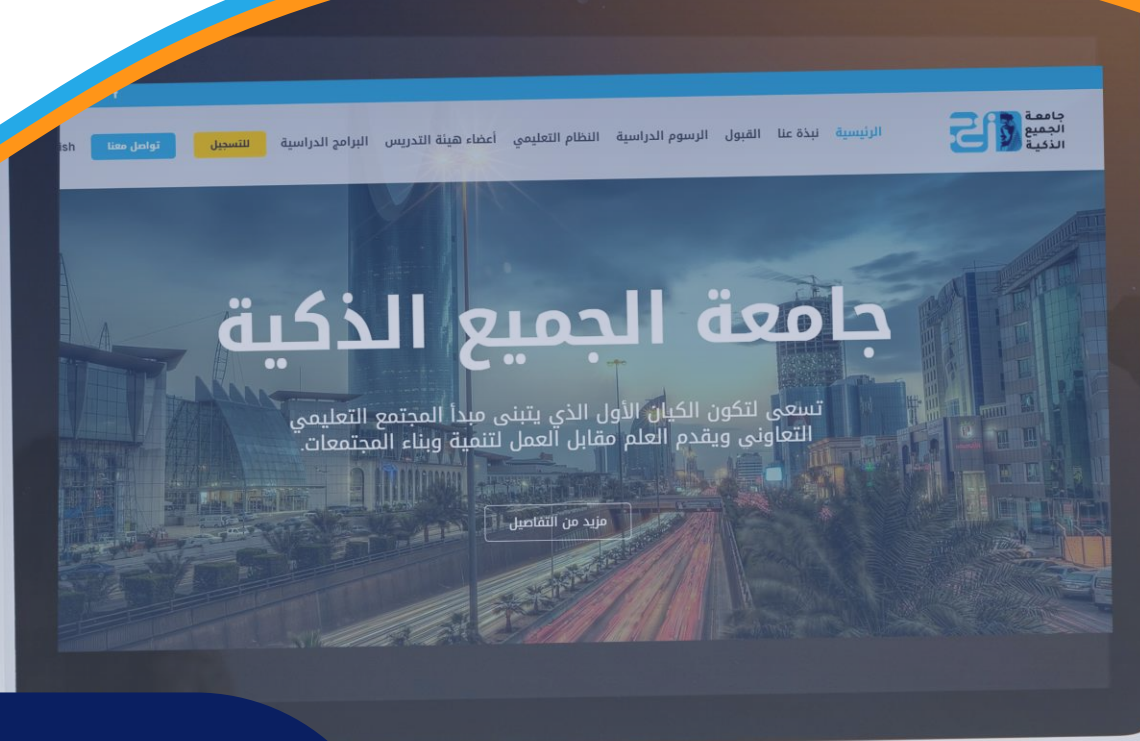




جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY



IoT Security
Prepared by Dr. Abdelrhman Ahmed
Lecture 7

Ensuring Privacy of IoT

IoT data collection is the process of using sensors to track the conditions of physical things. Devices and technology connected over the Internet of Things (IoT) can monitor and measure data in real-time. The data are transmitted, stored, and can be retrieved at any time.

IoT data has 3 main types:-

1. Equipment data:-

This type of data enables real-time fault detection, runtime-based schedules, and predictive maintenance thus saving energy costs, increasing productivity, and extending equipment life. Equipment data can be centralized in one platform so that on-site staff, management, and vendors can all be on the same page and data can roll up into executive dashboards.

2. Environmental data:-

IoT sensors can be deployed to track a range of data streams within buildings: temperature, air quality, people flow, moisture, or movement. These datasets are primarily used to be proactive for occupant comfort issues and avoid disaster scenarios such as leaks and floods.

3. Submeter data:-

Digital Submetering devices connected to the internet help automate the utility submetering process which costs, eliminates errors and generates bills as soon as the billing period ends. Submetering provides transparency to portfolio owners for the recovery rates of their cash outlays.

Several layers interplay to make the IoT data collection process work.

- Device Layer

In the IoT architecture, devices that communicate with each other form the primary layer. These devices include sensors that track environmental data, bluetooth devices, low-power radio-based devices, actuators, and so on.

IoT devices can be categorized under the following identities:

- A built-in chip-like unique identifier (or UUID) placed inside of a device;
- An identifier that depends on radio IoT data collection systems, for instance—Wi-Fi MAC, Bluetooth, and so forth.
- An identifier located inside the system's programmable non-volatile memory (EEPROM);
- A Refresh/Bearer token.

- **Event Processing Layer**

This layer processes and stores data collected from IoT devices. The event processing layer can be built via a database-powered server-side application like a JAX RS tool. You can also create this layer using IoT cloud services to process and store IoT data.

Other processes that occur in this layer include:

- data cleaning
- adding metadata to IoT data
- organizing data insights

- IT Edge Layer

This layer consists of the hardware, firmware, and operating system of your IoT devices. It's responsible for reading sensors attached to a device and changing the state of a device, say when a voice command is detected.

- Client Communication Layer

This layer transfers data from the device to the user. It acts as a bridge between back-end databases and front-end interfaces for end users of the data. This data gets out of the system through machine-to-machine APIs that relay IoT insights to an end-user via web or mobile application. For many reasons, all these intricate layers of technology come with several hurdles that companies need to overcome. Here are some of them.

- **Security**

Throughout the data collection, processing, and storage stages, security is a major concern. Because a lot of the data involved may be sensitive, substantial efforts have to be made to safeguard it from invasion.

- **Compatibility**

IoT systems widely vary in architecture and protocols. Many tools may not be able to support sensor data and information from custom Internet of Things (IoT) devices.



- **Large Data Sets**

IoT data collection typically involves capturing huge amounts of data streams. Moreover, this data has to be prepared for teams to gather some useful insights from it. This calls for the need for flexible strategies that optimize data collection, storage, preparation, and extrapolation.

- **Consistency**

It is costly to ensure consistent communication amongst devices on your IoT network. Other activities such as information processing, storage, and preemptive feedback procedures are not simple to run on a non-stop, daily basis.



Improve Data Collection To Reduce Privacy Concerns

- **Optimization of internal processes:** within a production line big data analysis is useful for managing the operation of the system and the prediction of criticality. For example, the data collected can help solve problems and failures able to block or damage the production and so develop solutions to avoid them.
- **Creation of new generations of products and services:** in the case of products, specific sensors allow to monitor of the operation of the devices and related components, while in the case of services it is possible to more enhance most required functions. These data allow to constantly develop products and services, to improve them or to create new solutions based on the usage behaviors. For example, Apps are able to adapt to customer's use and continually improve implementing some functions or leaving others.

- **Customization:** studying and interpreting the data produced by IoT it is possible to perform special tests and to intercept customer preferences. This is the case of a company that, analyzing the trends of use by the customers of a specific service, it provides new solutions to manage it even more effectively, basing precisely on its specific needs. Let's try to think of a current gas or water provider, having regard to the data of the consumption of a specific user (provided by IoT devices), which proposes rates or modeled offers according to specific customer usage trends.
- **Advertising and commerce:** the study of information allows to create customized advertising campaigns and strongly targeted. For example, within the context of e-commerce, the user can rediscover his preferences profiled through crossed information with the products of his research or with the historian of his purchases.

Improve Data Collection To Reduce Privacy Concerns

- **Direct monetization of data:** it is possible to earn through the sale of data to other external parties. The aggregated data from the IoT sensors of a private car parking for example, may be transferred to other entities in order to extrapolate relative trends about citizen car stops (number of cars, peak times, preferences between public and private car parks and much more).



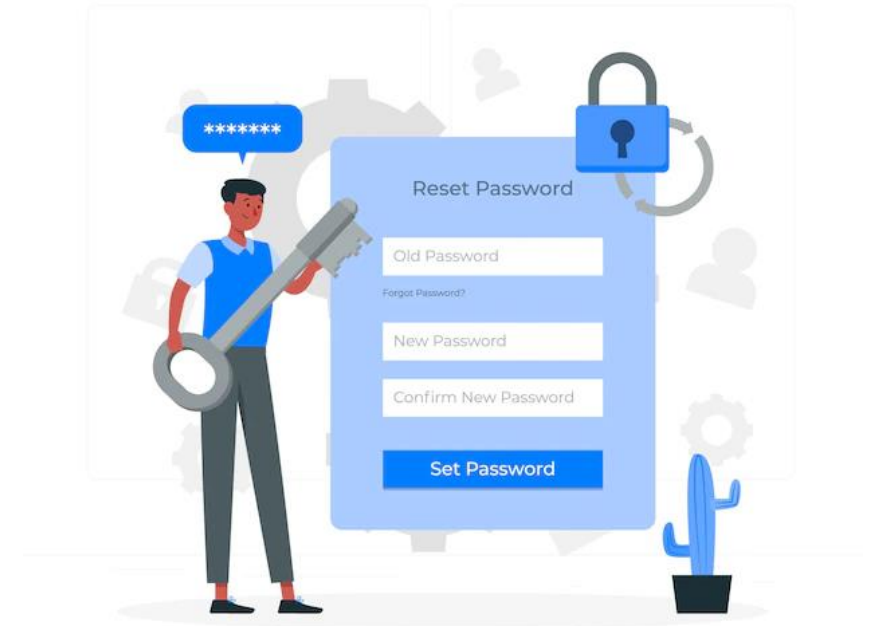
Ideally, securing data on IoT devices should be a doddle, if you ensure that your connected devices are secure by design. Unfortunately, for a number of reasons, this isn't always going to be possible. For this reason, five ways are listed that you can help to secure data on IoT devices.

1. Find Out How Many IoT Connected Devices You Have

When it comes to securing data on IoT connected devices, there is no more logical place to start than locating the number of IoT devices you actually have on your network. You need to know which types you have and what the devices are so that you can catalog any potential security vulnerabilities that your sensitive data may be exposed to. You should ensure that your list of connected devices is up to date and that you use it to segment your firewall policies.

2. Ensure Strict Password Policies

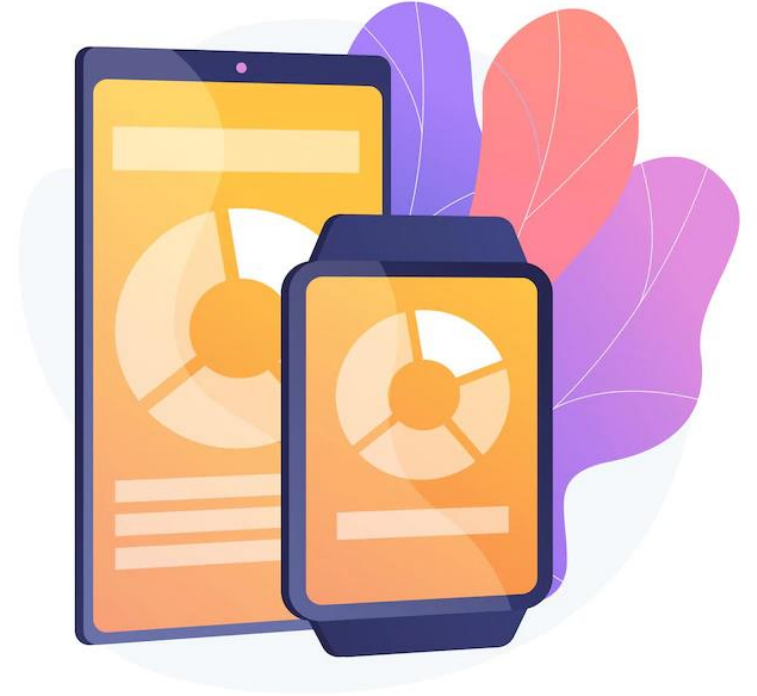
Compromised credentials frequently result in data breaches, and the same applies when we're discussing IoT connected devices. Implementing stringent password policies that include complex passwords that must be regularly updated, helps to take some of the risk away. As soon as any IoT device is connected to the network, its password should be changed immediately to something more in keeping with this new policy.



3. Keep Everything Up to Date

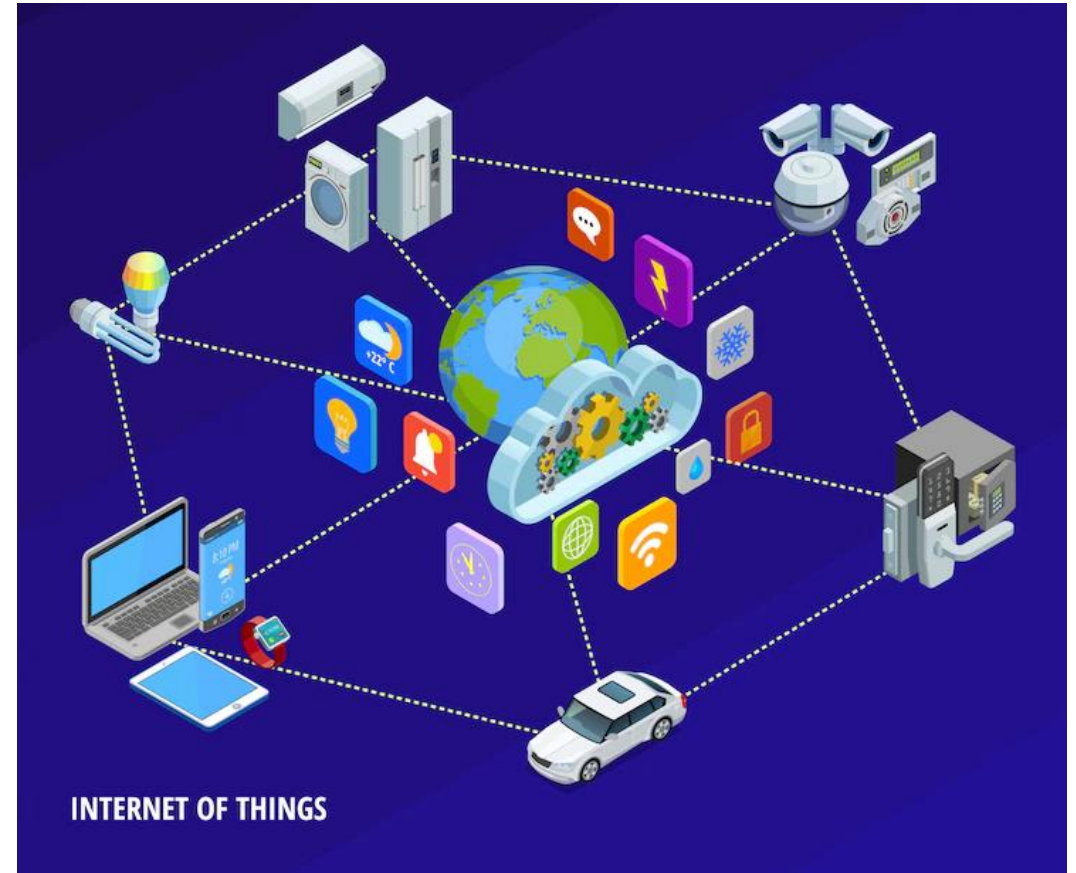
It should go without saying, but unfortunately many organizations and individuals do not keep their devices up to date. Most IT systems are regularly updated to help patch known security vulnerabilities, but IoT devices aren't often kept to the same standard. You need to ensure that users are actively going to the vendor website when setting up new IoT devices and downloading the latest security patches.

Establish a regular software update schedule to ensure that attackers cannot easily exploit known vulnerabilities in your systems.



4. Limit IoT Devices to Only the Useful Ones

When it comes to IoT devices, more does not necessarily mean better. Ensure you have analyzed the usefulness of each connected device and compared that to the security risks. Only implement IoT devices that you know will bring a tangible benefit to your business. Any IoT devices that aren't currently adding a benefit to your business should be disconnected.



5. Monitor Your Connected Devices

There are plenty of solutions out there that can analyze the behavior of all your network connected devices. When choosing a security solution that is designed to monitor how your sensitive data is being used on connected devices, ensure you pick one that can integrate with a more comprehensive Data Security Platform. That way, you can be sure that, wherever your sensitive data is located, you know where it is, who has access to it and what users are doing with it.



A Sound Destruction Policy in Place

When the hard drives or storage media reach the end of their operational lifespan, organizations should avoid haphazard release of IT assets to the secondhand market. Rather, form a zero-tolerance policy against the selling of used media without properly sanitizing them. Make sure your data destruction policy complies with all industry, state, and federal regulations. It must specifically define the length or period to preserve old data or devices, and preferred methods of secure data disposal. Consider conducting frequent reviews of your policies to incorporate revised guidelines and industry norms.

Define Data Eraser Protocol

Develop a protocol of securely erasing data before putting device to rest in a manner that employees do not compromise the underlying layer of security. Keep your staff educated about the potential harm careless disposal of devices can cause, if data is recovered or inadvertently fall into wrong hands. Moreover, get access to certified data eraser software to help your employees adopt automated data eraser practices instead of simply deleting or formatting the storage device. Such smart moves ensure unwanted data is permanently irretrievable. You may read our latest blog on 'Automate and Schedule Data Erasure Tasks To Maintain Privacy' & feel free to enlighten your staff through our informative piece.

Promote Employee Awareness

Each individual working from office or distributed location must be well-versed with the data destruction policy and meticulously observe it. Organizations must frequently conduct data destruction training and educational webinars for employees working from the office as a gentle reminder to sustain cyber hygiene. Random disposal of documents, drives (HDDs, SSDs etc.), or CDs in the trash bin should be strictly prohibited. The IT asset managers must take the responsibility to ensure data stored in the device that is no longer in use is permanently wiped and the certificate of erasure is religiously maintained as a proof of erasure to meet compliance.

Reassess Sanitization Process

Conventional media sanitization procedures are no longer applicable to the modern/advanced flash memory-based devices. The new storage devices and technologies are vividly distinct from the legacy magnetic media and require redefining of data destruction process to ensure efficacy of data sanitization. Destruction without media sanitization should be considered only in rare conditions when the device is inaccessible for overwriting process and needs to be physically destructed. It is the responsibility of the IT asset manager and data controller to find the most suitable data destruction method to recycle modern drives and devices.

Backup Destruction is Compulsory

Many organizations keep multiple backup files, folders, or data banks to thwart the possibility of accidentally losing confidential information. If primary data sources are disposed, their backups should be wiped off too. Overlooking the process or inadequately dumping the backup tapes is equally unethical and may cause serious repercussions to the enterprise.

Maintain Chain of Custody Records

A worthwhile chain of custody covers an auditable digital or document trail. It must also include an inclusive history of all the people who held the devices, stored, or transported them. Leave no room for error otherwise even an improper chain of custody can cause disposal concerns with fines, legal ramifications, auditors' censure and, brand disrepute.

Demand Certificate of Destruction

A Certificate of Destruction is an audit document that affirms successful destruction of confidential data stored on hard drives, tapes, SSDs, or other storage media. Certificate of erasure ensures that you have actually destroyed the data in lines with the mandates of global data privacy and data protection. Hence, organization must use tools or hire service providers that offer Certificate of Destruction as a proof to have permanently destroyed data. It is a resilient approach that ensure that data is no longer exposed to bad actors and prevents any lapse or data breach risk.

1. Erase all data and personal information. The manufacturer should provide a method for how to erase your data and personal information from both the device and associated applications. Erasing your personal information ensures that no-one gains access to it after you have disposed of the device. Delete your online account if it is no longer needed without the IoT device.
2. Perform a factory reset of the device. A factory reset is designed to erase data kept in local storage and reset usernames, passwords and settings back to default. Check the device's user manual or the manufacturer's website for information on how to perform a factory reset.

3. Disassociate the device from mobile phones and other devices. Disposing of a device that still has access to your other devices, network or online accounts has the potential for others to gain access. Make sure you check your other devices and remove any pairing with the device you are disposing of. Remove any permissions granted to the mobile application that are no longer needed.
4. Remove any removable media (e.g. USB flash drives, memory cards etc) attached to the device. Removable media may contain personal data that is not deleted in a factory reset and should be physically removed, physically destroyed and disposed of separately from the device.